II

(Nelegislativní akty)

ROZHODNUTÍ

PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2022/254

ze dne 17. prosince 2021

podle nařízení Evropského parlamentu a Rady (EU) 2016/679 týkající se odpovídající ochrany osobních údajů poskytované Korejskou republikou na základě zákona o ochraně osobních údajů

(oznámeno pod číslem C(2021) 9316)

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) ([1]), a zejména na čl. 45 odst. 3 uvedeného nařízení,

vzhledem k těmto důvodům:

1. ÚVOD

(1) Nařízení (EU) 2016/679 stanoví pravidla pro předávání osobních údajů správci nebo zpracovateli v Unii do třetích zemí a mezinárodním organizacím, pokud toto předávání spadá do oblasti působnosti uvedeného nařízení. Pravidla pro mezinárodní předávání údajů stanoví kapitola V (články 44 až 50) uvedeného nařízení. Jakkoli je tok osobních údajů do zemí a ze zemí mimo Evropskou unii nezbytný pro rozvoj přeshraničního obchodu a mezinárodní spolupráce, úroveň ochrany osobních údajů v Unii nesmí být předáváním těchto údajů do třetích zemí oslabena ([2]).

(2) Podle čl. 45 odst. 3 nařízení (EU) 2016/679 může Komise prostřednictvím prováděcího aktu rozhodnout, že určitá třetí země, určité území či jedno nebo více konkrétních odvětví v určité třetí zemi nebo určitá mezinárodní organizace zajišťuje odpovídající úroveň ochrany. Za této podmínky se může předávání osobních údajů do třetí země bez nutnosti získat další povolení uskutečnit, jak stanoví čl. 45 odst. 1 a 103. bod odůvodnění nařízení (EU) 2016/679.

(3) Podle čl. 45 odst. 2 nařízení (EU) 2016/679 musí přijetí rozhodnutí o odpovídající ochraně vycházet z komplexní analýzy právního řádu dané třetí země, a to jak z hlediska pravidel použitelných pro dovozce údajů, tak z hlediska omezení a záruk vztahujících se k přístupu orgánů veřejné správy osobním údajům. V tomto posouzení musí Komise určit, zda daná třetí země zaručuje úroveň ochrany „v zásadě rovnocennou“ úrovni ochrany zajištěné v Evropské unii (104. bod odůvodnění nařízení (EU) 2016/679). To, zda tomu tak je, musí být posouzeno podle právních předpisů Unie, a to zejména nařízení (EU) 2016/679, jakož i judikatury Soudního dvora Evropské unie ([3]).

([1]) Úř. věst. L 119, 4.5.2016, s. 1.
([2]) Viz 101. bod odůvodnění nařízení (EU) 2016/679.
([3]) Nejnověji viz věc C-311/18, Facebook Ireland a Schrems (dále jen „rozsudek ve věci Schrems II“), ECLI:EU:C:2020:559.

(4) Jak objasnil Soudní dvůr Evropské unie, nevyžaduje to zjištění stejné úrovně ochrany ([4]). Zejména prostředky, které dotyčná třetí země k ochraně osobních údajů využívá, se mohou lišit od prostředků zavedených v Unii, pokud se v praxi ukážou jako účinné k zajištění odpovídající úrovně ochrany ([5]). Standard odpovídající ochrany tedy nevyžaduje opakování pravidel Unie slovo od slova. Kritériem je spíše to, zda zahraniční systém jako celek zajišťuje prostřednictvím podstaty práva na soukromí a jeho účinného uplatňování, dozoru a vymáhání požadovanou úroveň ochrany ([6]). Vodítko v tomto ohledu nabízí i referenční rámec pro odpovídající ochranu stanovený Evropským sborem pro ochranu osobních údajů, který má tento standard dále vyjasnit ([7]).

(5) Komise pečlivě analyzovala korejské právní předpisy a praxi. Na základě zjištění uvedených v 8. až 208. bodě odůvodnění dospěla Komise k závěru, že Korejská republika zajišťuje odpovídající úroveň ochrany osobních údajů předávaných správcem nebo zpracovatelem v Unii ([8]) subjektům v Koreji (např. fyzickým nebo právnickým osobám, organizacím, veřejným institucím), které spadají do oblasti působnosti zákona o ochraně osobních údajů (zákon č. 10465 ze dne 29. března 2011 naposledy pozměněný zákonem č. 16930 ze dne 4. února 2020). To zahrnuje správce i zpracovatele údajů (nazývané „externí subjekty zajišťující zpracování“ ([9])) ve smyslu nařízení (EU) 2016/679. Toto zjištění o odpovídající úrovni ochrany nezahrnuje zpracování osobních údajů náboženskými organizacemi pro misijní činnost a zpracování osobních údajů politickými stranami pro nominaci kandidátů ani zpracování osobních úvěrových informací podle zákona o úvěrových informacích správci údajů, kteří podléhají dozoru ze strany Komise pro finanční služby.

(6) Tento závěr zohledňuje další záruky stanovené v oznámení č. 2021-5 (příloha I) a oficiální prohlášení, ujištění a závazky korejské vlády vůči Komisi (příloha II).

(7) Toto rozhodnutí má účinek v tom smyslu, že předávání údajů správcům a zpracovatelům osobních údajů v Korejské republice může probíhat, aniž by bylo nutné získat další povolení. Tímto rozhodnutím není dotčeno přímé uplatňování nařízení (EU) 2016/679 na takové subjekty, pokud jsou splněny podmínky týkající se místní působnosti uvedeného nařízení, stanovené v jeho článku 3.

2. PRAVIDLA TÝKAJÍCÍ SE ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

2.1 Rámec zpracování osobních údajů v Korejské republice

(8) Právní systém upravující ochranu soukromí a údajů v Koreji se opírá o korejskou ústavu vyhlášenou dne 17. července 1948. Ačkoli právo na ochranu osobních údajů není v ústavě výslovně stanoveno, je nicméně uznáváno jako základní právo odvozené z ústavních práv na lidskou důstojnost a usilování o štěstí (článek 10), soukromý život (článek 17) a důvěrnost komunikací (článek 18). To potvrzuje Nejvyšší soud ([10]) i Ústavní soud ([11]). Základní práva a svobody (včetně práva na soukromí) mohou být omezeny pouze zákonem, je-li to nezbytné pro národní bezpečnost nebo pro zachování práva a pořádku v zájmu veřejného blaha, a toto omezení se nesmí dotýkat podstaty dotčené svobody nebo práva (čl. 37 odst. 2).

([4]) Věc C-362/14, Maximillian Schrems v. Data Protection Commissioner (dále jen „rozsudek ve věci Schrems“), ECLI:EU:C:2015:650, bod 73.

([5]) Rozsudek ve věci Schrems, bod 74.

([6]) Viz sdělení Komise Evropskému parlamentu a Radě, Výměna a ochrana osobních údajů v globalizovaném světě, COM(2017) 7, 10.1.2017, oddíl 3.1, s. 6–7.

([7]) Evropský sbor pro ochranu osobních údajů, Referenční rámec pro odpovídající ochranu, WP 254 rev. 01, k dispozici na této adrese: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([8]) Toto rozhodnutí má význam pro EHP. Dohoda o Evropském hospodářském prostoru (Dohoda o EHP) stanoví rozšíření vnitřního trhu Evropské unie o tři státy EHP, a to Island, Lichtenštejnsko a Norsko. Rozhodnutí Smíšeného výboru, kterým se do přílohy XI Dohody o EHP začleňuje nařízení (EU) 2016/679, přijal Smíšený výbor EHP dne 6. července 2018 a v platnost vstoupilo dne 20. července 2018. Uvedená dohoda se tedy na nařízení vztahuje. Pro účely tohoto rozhodnutí se tudíž odkazy na EU a členské státy EU vykládají jako odkazy zahrnující i státy EHP.

([9]) Viz oddíl 2.2.3 tohoto rozhodnutí.

([10]) Viz například rozhodnutí Nejvyššího soudu 2014Da77970, 15. října 2015 (shrnutí v anglickém jazyce je k dispozici pod odkazem „Lawmaker's disclosure of teachers' trade union members case“ (Zveřejnění zákonodárce týkající se členů učitelských odborů) na adrese https://www.privacy.go.kr/eng/enforcement_01.do) a zde citovaná judikatura včetně rozhodnutí 2012Da49933, 24. července 2014.

([11]) Viz zejména rozhodnutí Ústavního soudu 99Hun-ma513, 26. května 2005 (shrnutí v anglickém jazyce je k dispozici na odkazu http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) a rozhodnutí 2014JHun-ma449 2013 Hun-Ba68 (konsolidované znění), 23. prosince 2015 (shrnutí v anglickém jazyce je k dispozici pod odkazem „Change of resident registration number case“ (Změna registračního čísla rezidenta) na adrese https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Přestože ústava na různých místech odkazuje na práva korejských občanů, Ústavní soud rozhodl, že i cizí státní příslušníci mají základní práva ([12]). Konkrétně tento soud konstatoval, že ochrana důstojnosti a hodnoty člověka jako lidské bytosti, jakož i právo usilovat o štěstí jsou právy každé lidské bytosti, nejen občanů ([13]). Podle oficiálních prohlášení korejské vlády ([14]) se navíc obecně uznává, že články 12 až 22 ústavy (které zahrnují práva na soukromí) stanoví základní lidská práva ([15]). Ačkoli dosud neexistuje judikatura, která by se konkrétně týkala práva cizích státních příslušníků na soukromí, základ tohoto práva spočívající v ochraně lidské důstojnosti a usilování o štěstí tento závěr podporuje ([16]).

(10) Kromě toho Korea přijala řadu právních předpisů v oblasti ochrany údajů, které poskytují záruky pro všechny jednotlivce bez ohledu na jejich státní příslušnost ([17]). Pro účely tohoto rozhodnutí jsou relevantními zákony:

— zákon o ochraně osobních údajů,

— zákon o používání a ochraně úvěrových informací ([18]),

— zákon o ochraně důvěrnosti komunikací.

(11) Zákon o ochraně osobních údajů poskytuje obecný právní rámec ochrany údajů v Korejské republice. Je doplněn prováděcí vyhláškou (prezidentská vyhláška č. 23169 ze dne 29. září 2011, ve znění prezidentské vyhlášky č. 30892 ze dne 4. srpna 2020) (dále jen „prováděcí vyhláška k zákonu o ochraně osobních údajů“), která je stejně jako zákon o ochraně osobních údajů právně závazná a vymahatelná.

(12) Další pravidla pro výklad a použití zákona o ochraně osobních údajů obsahují i regulační „oznámení“ přijatá Komisí pro ochranu osobních údajů. Na základě článku 5 (Povinnosti státu) a článku 14 zákona o ochraně osobních údajů (Mezinárodní spolupráce) přijala Komise pro ochranu osobních údajů oznámení č. 2021-5 ze dne 1. září 2020 (ve znění oznámení č. 2021-1 ze dne 21. ledna 2021 a oznámení č. 2021-5 ze dne 16. listopadu 2021, dále jen „oznámení č. 2021-5“) o výkladu, uplatňování a prosazování některých ustanovení zákona o ochraně osobních údajů. Toto oznámení uvádí vysvětlení, která se vztahují na jakékoli zpracování osobních údajů podle zákona o ochraně osobních údajů, jakož i další záruky pro osobní údaje předávané do Koreje na základě tohoto rozhodnutí. Oznámení je právně závazné pro správce osobních údajů a vymahatelné ze strany Komise pro ochranu osobních údajů i soudů ([19]). Porušení pravidel uvedených v oznámení znamená porušení příslušných ustanovení zákona o ochraně osobních údajů, která pravidla doplňují. Obsah dalších záruk je proto analyzován jako součást posouzení příslušných článků zákona o ochraně osobních údajů. A konečně další pokyny k zákonu o ochraně osobních údajů a jeho prováděcí vyhlášce, které upřesňují uplatňování a prosazování pravidel ochrany údajů Komisí pro ochranu osobních údajů, jsou uvedeny v příručce a pokynech k zákonu o ochraně osobních údajů, které přijala Komise pro ochranu osobních údajů ([20]).

([12]) Rozhodnutí Ústavního soudu 93 Hun-MA120, 29. prosince 1994.
([13]) Rozhodnutí Ústavního soudu 99HeonMa494, 29. listopadu 2001.
([14]) Viz oddíl 1.1 přílohy II.
([15]) Viz rovněž článek 1 zákona o ochraně osobních údajů, který výslovně uvádí „svobody a práva jednotlivců“. Konkrétněji uvádí, že účelem takového zákona je „stanovit zpracování a ochranu osobních údajů pro účely ochrany svobody a práv fyzických osob a další realizace důstojnosti a hodnoty jednotlivců“. Podobně čl. 5 odst. 1 zákona o ochraně osobních údajů stanoví povinnost státu „formulovat zásady, které mají zabránit škodlivým důsledkům shromažďování údajů za jiným než určeným účelem, zneužívání a neoprávněného užívání osobních údajů, indiskrétního dohledu a sledování atd. a posílit důstojnost lidských bytostí a soukromí jednotlivců“.
([16]) Kromě toho čl. 6 odst. 2 ústavy stanoví, že postavení cizinců je zaručeno v souladu s mezinárodním právem a úmluvami. Korea je smluvní stranou několika mezinárodních dohod, které zaručují právo na soukromí, jako je Mezinárodní pakt o občanských a politických právech (článek 17), Úmluva o právech osob se zdravotním postižením (článek 22) a Úmluva o právech dítěte (článek 16).
([17]) To zahrnuje pravidla, která jsou relevantní pro ochranu osobních údajů, neplatí však v situaci, kdy jsou osobní údaje shromažďovány v Unii a předávány do Koreje podle nařízení (EU) 2016/679, například ustanovení zákona o ochraně, používání a jiném nakládání s údaji o poloze.
([18]) Účelem tohoto zákona je podpořit řádné podnikání v oblasti úvěrových informací, prosazovat účinné využívání a systematickou správu úvěrových informací a chránit soukromí před zneužitím a neoprávněným použitím úvěrových informací (článek 1 zákona).
([19]) Korejské soudy například rozhodovaly v řadě případů o souladu s regulačními oznámeními, mimo jiné vydaly rozhodnutí o odpovědnosti korejských správců údajů za porušení oznámení (viz např. rozhodnutí Nejvyššího soudu 2018Da219406 ze dne 25. října 2018, v němž soud správci údajů nařídil, aby vyplatil fyzickým osobám náhradu škody utrpěné v důsledku porušení „Oznámení o normách pro opatření k zajištění bezpečnosti osobních informací“; viz rovněž rozhodnutí Nejvyššího soudu 2018Da219352, 25. října 2018, rozhodnutí Nejvyššího soudu 2011Da24555, 16. května 2016, rozhodnutí soudu prvního stupně pro Seoul Central District 2014Gahap511956, 13. října 2016, rozhodnutí soudu prvního stupně pro Seoul Central District 2009Gahap43176, 26. ledna 2010).
([20]) Ustanovení čl. 12 odst. 1 zákona o ochraně osobních údajů.

(13) Zákon o používání a ochraně úvěrových informací dále stanoví specifická pravidla, která se vztahují na „běžné“ komerční subjekty i na specializované subjekty ve finančním sektoru, pokud zpracovávají osobní úvěrové informace, tj. informace, které jsou nezbytné pro zjištění úvěruschopnosti účastníků finančních nebo obchodních transakcí. To zahrnuje zejména jméno, kontaktní údaje, finanční transakce, úvěrový rating, stav pojištění nebo zůstatek úvěru, jsou-li tyto informace použity k určení úvěruschopnosti jednotlivce ([21]). Naopak tam, kde jsou takové údaje použity pro jiné účely (např. lidské zdroje), se v plném rozsahu použije zákon o ochraně osobních údajů. Pokud jde o zvláštní ustanovení zákona o používání a ochraně úvěrových informací týkajících se ochrany údajů, zajišťuje dozor zčásti Komise pro ochranu osobních údajů (pro komerční organizace viz článek 45-3 zákona o používání a ochraně úvěrových informací) a zčásti Komise pro finanční služby ([22]) (pro finanční sektor včetně ratingových agentur, bank, pojišťoven, vzájemných spořitelen, specializovaných finančních úvěrových společností, společností poskytujících finanční investiční služby, společností zajišťujících financování cenných papírů, úvěrových družstev atd., viz čl. 45 odst. 1 zákona o používání a ochraně úvěrových informací ve spojení s článkem 36-2 prováděcí vyhlášky k uvedenému zákonu a s článkem 38 zákona o Komisi pro finanční služby). V tomto ohledu je oblast působnosti tohoto rozhodnutí omezena na komerční subjekty, které podléhají dozoru Komise pro ochranu osobních údajů ([23]). Zvláštní pravidla zákona o používání a ochraně úvěrových informací, která platí v této souvislosti (obecná pravidla zákona o ochraně osobních údajů platí tam, kde neexistují žádná zvláštní pravidla), jsou popsána v oddíle 2.3.11.

2.2 **Věcná a osobní působnost zákona o ochraně osobních údajů**

(14) Není-li v jiných zákonech výslovně stanoveno jinak, řídí se ochrana osobních údajů zákonem o ochraně osobních údajů (článek 6). Věcná a osobní působnost jeho použití je dána definovanými pojmy „osobní údaje“, „zpracování“ a „správce osobních údajů“.

2.2.1 *Definice osobních údajů*

(15) Ustanovení čl. 2 odst. 1 zákona o ochraně osobních údajů definuje osobní údaje jako údaje týkající se žijící fyzické osoby, které tuto fyzickou osobu identifikují buď přímo, například její jméno, registrační číslo rezidenta nebo fotografie, nebo nepřímo, jmenovitě pokud lze údaje, které samy o sobě nemohou určitou osobu identifikovat, snadno zkombinovat s dalšími údaji. Skutečnost, zda lze údaje „snadno“ zkombinovat, závisí na tom, zda je taková kombinace přiměřeně pravděpodobná s přihlédnutím k možnosti získat další údaje, jakož i k času, nákladům a technologii potřebným k identifikaci fyzické osoby.

(16) Kromě toho se pseudonymizované údaje (tedy údaje, které nemohou identifikovat konkrétní fyzickou osobu, aniž by byly použity nebo zkombinovány s dalšími údaji za účelem uvedení do původního stavu) podle zákona o ochraně osobních údajů považují za osobní údaje (čl. 2 odst. 1 písm. c) zákona o ochraně osobních údajů). Naopak údaje, které jsou plně „anonymizovány“, jsou z oblasti působnosti zákona o ochraně osobních údajů vyňaty (článek 58-2 zákona o ochraně osobních údajů). Jedná se o údaje, které nemohou identifikovat konkrétní fyzickou osobu, i pokud jsou zkombinovány s jinými údaji, a to s přihlédnutím k možnosti získat další údaje, jakož i k času, nákladům a technologii potřebným k identifikaci.

(17) To odpovídá věcné oblasti působnosti nařízení (EU) 2016/679 a jeho pojmům „osobní údaje“, „pseudonymizace“ ([24]) a „anonymizované údaje“ ([25]).

([21]) Ustanovení čl. 2 odst. 1 zákona o používání a ochraně úvěrových informací.

([22]) Komise pro finanční služby je korejským dozorovým úřadem pro finanční sektor a v této funkci také prosazuje zákon o používání a ochraně úvěrových informací.

([23]) Pokud by v budoucnu došlo ke změně, např. rozšířením jurisdikce Komise pro ochranu osobních údajů na veškeré zpracování osobních úvěrových informací v rámci zákona o používání a ochraně úvěrových informací, by bylo možné zvážit změnu rozhodnutí o odpovídající ochraně, tak aby se toto rozhodnutí vztahovalo také na subjekty, které v současnosti podléhají dozoru Komise pro finanční služby.

([24]) V zákoně o ochraně osobních údajů se za „pseudonymní zpracování“ považuje zpracování metodami, jako je částečné vymazání osobních údajů nebo částečné nebo úplné nahrazení osobních údajů takovým způsobem, že bez dalších informací nelze rozpoznat žádnou konkrétní fyzickou osobu (čl. 2 odst. 1-2) zákona o ochraně osobních údajů). To odpovídá definici pseudonymizace podle čl. 4 bodu 5 nařízení (EU) 2016/679, který uvádí „zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné osobě“.

([25]) Konkrétně 26. bod odůvodnění nařízení (EU) 2016/679 objasňuje, že nařízení se nevztahuje na anonymizované informace, totiž informace, které se netýkají identifikované či identifikovatelné fyzické osoby. Toto určení pak závisí na všech prostředcích, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou či nepřímou identifikaci dané fyzické osoby. Ke stanovení toho, zda lze rozumně předpokládat použití takových prostředků, musí být vzaty v úvahu všechny objektivní faktory, jako jsou náklady a čas, které si identifikace vyžádá, s přihlédnutím k technologii dostupné v době zpracování i k technologickému rozvoji.

2.2.2 *Definice zpracování*

(18) Pojem „zpracování“ je v zákoně o ochraně osobních údajů definován široce jako „shromažďování, generování, spojování, propojování, zaznamenávání, ukládání, uchovávání, zpracování s přidanou hodnotou, editace, vyhledávání, výstup, oprava, obnova, použití, poskytování, zveřejňování a ničení osobních údajů a jiné podobné činnosti“ ([26]). Ačkoli některá ustanovení zákona o ochraně osobních údajů odkazují pouze na konkrétní druhy zpracování, jako je „používání“, „poskytnutí“ nebo „shromažďování“ ([27]), pojem „použití“ je vykládán tak, že zahrnuje jakýkoli druh zpracování jiný než „shromažďování“ nebo „poskytování“ (třetí straně). Tento široký výklad pojmu „používání“ tak zajišťuje, že v ochraně neexistují žádné mezery, pokud jde o konkrétní činnosti zpracování. Pojem zpracování tedy odpovídá stejnému pojmu podle nařízení (EU) 2016/679.

2.2.3 *Správce osobních údajů a „externí subjekt zajišťující zpracování“*

(19) Zákon o ochraně osobních údajů se vztahuje na „správce osobních údajů“ (dále jen „správce“). Obdobně jako v nařízení (EU) 2016/679 tento pojen zahrnuje jakoukoli veřejnou instituci, právnickou osobu, organizaci nebo fyzickou osobu, která v rámci své činnosti přímo či nepřímo zpracovává osobní údaje za účelem používání souborů osobních údajů ([28]). V této souvislosti se „souborem osobních údajů“ rozumí jakýkoli „soubor nebo soubory osobních údajů systematicky uspořádané nebo organizované na základě určitého pravidla pro snadný přístup k osobním údajům“ (čl. 2 odst. 4 zákona o ochraně osobních údajů) ([29]). Interně je správce povinen vyškolit osoby zapojené do zpracování pod jeho vedením, jako jsou vedoucí pracovníci nebo zaměstnanci společnosti, a provádět náležitou kontrolu a dohled (čl. 28 odst. 1 zákona o ochraně osobních údajů).

(20) Specifické povinnosti se vztahují na případy, kdy správce („zadavatel zpracování“) zadá zpracování osobních údajů třetí straně („externí subjekt zajišťující zpracování“). Zajišťování externího zpracování se musí zejména řídit právně závazným ujednáním (obvykle smlouvou) ([30]), jež stanoví rozsah externě zajišťovaných prací, účel zpracování, technické a řídicí záruky, které mají být použity, dohled ze strany správce, odpovědnost (např. náhradu škody způsobené porušením smluvních povinností), jakož i omezení jakéhokoli dílčího zpracování ([31]) (čl. 26 odst. 1 a 2 zákona o ochraně osobních údajů ve spojení s čl. 28 odst. 1 prováděcí vyhlášky) ([32]).

(21) Kromě toho musí správce zveřejňovat a průběžně aktualizovat podrobnosti o činnosti zadané externímu subjektu zajišťujícímu zpracování a jeho totožnosti, nebo přímo oznamovat příslušné údaje v rozsahu, v jakém se externí zpracování týká činností přímého marketingu, fyzickým osobám (čl. 26 odst. 2 a 3 zákona o ochraně osobních údajů ve spojení s čl. 28 odst. 2 až 5 prováděcí vyhlášky) ([33]).

(22) Dále je správce podle čl. 26 odst. 4 zákona o ochraně osobních údajů ve spojení s čl. 28 odst. 6 prováděcí vyhlášky povinen „poučit“ externí subjekt zajišťující zpracování o nezbytných bezpečnostních opatřeních a dohlížet, a to i prostřednictvím inspekcí, zda subjekt plní všechny povinnosti správce podle zákona o ochraně osobních údajů ([34]) i podle smlouvy o zajištění externího zpracování. Pokud externí subjekt zajišťující zpracování způsobí škodu v důsledku porušení zákona o ochraně osobních údajů, budou jeho jednání nebo nečinnost pro účely odpovědnosti přičteny správci stejně jako v případě zaměstnance (čl. 26 odst. 6 zákona o ochraně osobních údajů).

([26]) Ustanovení čl. 2 odst. 2 zákona o ochraně osobních údajů.

([27]) Například články 15 až 19 zákona o ochraně osobních údajů uvádějí pouze shromažďování, používání a poskytování osobních údajů.

([28]) Ustanovení čl. 2 odst. 5 zákona o ochraně osobních údajů. Veřejné instituce ve smyslu zákona o ochraně osobních údajů zahrnují všechny ústřední správní útvary nebo úřady a jejich přidružené subjekty, místní samosprávy, školy a veřejné korporace s investicemi orgánů místní správy, správní orgány Národního shromáždění a soudy (včetně Ústavního soudu) (čl. 2 odst. 6 zákona o ochraně osobních údajů ve spojení s článkem 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

([29]) To odpovídá oblasti věcné působnosti nařízení (EU) 2016/679. Podle čl. 2 odst. 1 nařízení (EU) 2016/679 se nařízení vztahuje na „zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny“. Ustanovení čl. 4 bodu 6 nařízení (EU) 2016/679 definuje „evidenci“ jako „jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií“. V souladu s tím 15. bod odůvodnění vysvětluje, že ochrana fyzických osob by se měla vztahovat „jak na automatizované zpracování osobních údajů, tak na manuální zpracování, pokud jsou tyto údaje uloženy v evidenci nebo do ní mají být vloženy. Záznamy nebo soubory záznamů ani jejich titulní strany, které nejsou uspořádány podle určených hledisek, by do oblasti působnosti tohoto nařízení spadat neměly“.

([30]) Viz příručka k zákonu o ochraně osobních údajů, kapitola III oddíl 2 k článku 26 (s. 203–212), která vysvětluje, že čl. 26 odst. 1 zákona o ochraně osobních údajů odkazuje na závazná ujednání, jako jsou smlouvy nebo obdobná ujednání.

([31]) Podle čl. 26 odst. 5 zákona o ochraně osobních údajů nesmí zpracovatel používat žádné osobní údaje nad rámec externě zajišťované činnosti nebo poskytovat osobní údaje třetí osobě. Nedodržení tohoto požadavku může vést k trestnímu postihu podle čl. 71 bodu 2 zákona o ochraně osobních údajů.

([32]) Nesplnění tohoto požadavku může vést k uložení pokuty, viz čl. 75 odst. 4 bod 4 zákona o ochraně osobních údajů.

([33]) Nesplnění tohoto požadavku může vést k uložení pokuty, viz čl. 75 odst. 2 bod 1 a odst. 4 bod 5 zákona o ochraně osobních údajů.

([34]) Viz také čl. 26 odst. 7 zákona o ochraně osobních údajů, podle kterého se na zpracovatele obdobně použijí články 15 až 25, 27 až 31, 33 až 38 a 50.

(23) Ačkoli tedy zákon o ochraně osobních údajů nepoužívá různé pojmy pro „správce“ a „zpracovatele“, pravidla pro zajišťování externího zpracování poskytují v zásadě rovnocenné povinnosti a záruky jako pravidla, které upravují vztah mezi správci a zpracovateli podle nařízení (EU) 2016/679.

2.2.4 *Zvláštní ustanovení pro poskytovatele informačních a komunikačních služeb*

(24) Zákon o ochraně osobních údajů se použije na zpracování osobních údajů kterýmkoli správcem, některá ustanovení však obsahují zvláštní pravidla (jakožto *lex specialis*) pro zpracování osobních údajů „uživatelů“ „poskytovateli informačních a komunikačních služeb“ ([35]). Pojem „uživatelé“ zahrnuje fyzické osoby, které využívají informační a komunikační služby (čl. 2 odst. 1 bod 4 zákona o podpoře využívání informačních a komunikačních sítí a ochraně údajů, dále jen „zákon o sítích“). To vyžaduje, aby fyzická osoba buď přímo využívala telekomunikační služby poskytované korejským poskytovatelem telekomunikačních služeb, nebo využívala informační služby ([36]) poskytované komerčně (tj. za účelem zisku) subjektem, který naopak využívá služby poskytovatele telekomunikačních služeb s licencí/registrací v Koreji ([37]). V obou případech je subjektem vázaným konkrétními ustanoveními zákona o ochraně osobních údajů subjekt, který nabízí on-line službu přímo fyzické osobě (tj. uživateli).

(25) Naopak zjištění o odpovídající úrovni ochrany se týká výhradně úrovně ochrany poskytované osobním údajům předávaným správcem/zpracovatelem v Unii subjektu v třetí zemi (zde: v Korejské republice). V posledně uvedeném scénáři budou mít jednotlivci v Unii obvykle přímý vztah pouze s „vývozcem údajů“ v Unii, nikoli s korejským poskytovatelem informačních a komunikačních služeb ([38]). Zvláštní ustanovení zákona o ochraně osobních údajů týkající se osobních údajů uživatelů informačních a komunikačních služeb se proto budou na osobní údaje předávané podle tohoto rozhodnutí vztahovat nanejvýš v omezených situacích.

2.2.5 *Výjimka z určitých ustanovení zákona o ochraně osobních údajů*

(26) Ustanovení čl. 58 odst. 1 zákona o ochraně osobních údajů vylučuje použití části zákona o ochraně osobních údajů (tj. článků 15 až 57), pokud jde o čtyři kategorie zpracování údajů ([39]). Nepoužijí se zejména části zákona o ochraně osobních údajů týkající se zvláštních důvodů zpracování, některých povinností v oblasti ochrany údajů, podrobných pravidel pro výkon individuálních práv a také pravidel pro řešení sporů mediačním výborem pro spory týkající se osobních údajů. Ostatní základní ustanovení zákona o ochraně osobních údajů zůstávají použitelná, zejména obecná ustanovení o zásadách ochrany údajů (článek 3 zákona o ochraně osobních údajů), včetně například zásad zákonnosti, specifikace účelu a účelového omezení, minimalizace údajů, přesnosti a zabezpečení údajů, a o individuálních právech (např. na přístup, opravu, výmaz a pozastavení zpracování, viz článek 4 zákona o ochraně osobních údajů). Kromě toho čl. 58 odst. 4 zákona o ochraně osobních údajů ukládá pro tyto činnosti zpracování specifické povinnosti, zejména pokud jde o minimalizaci údajů, omezené uchovávání údajů, bezpečnostní opatření a vyřizování stížností ([40]). V důsledku toho by jednotlivci mohli podat stížnost Komisi pro ochranu osobních údajů, pokud by tyto zásady a povinnosti nebyly dodržovány, a Komise pro ochranu osobních údajů je v případě nedodržení uvedených zásad a povinností oprávněna přijmout donucovací opatření.

([35]) Viz zejména čl. 18 odst. 2 a kapitola VI zákona o ochraně osobních údajů.

([36]) Informační služby zahrnují jak poskytování informací, tak zprostředkovatelské služby pro poskytování informací.

([37]) Viz čl. 2 odst. 1 bod 3 (ve spojení s čl. 2 odst. 1 body 2 a 4) zákona o sítích a čl. 2 odst. 6 a 8 zákona o telekomunikačních službách.

([38]) Pokud by korejští poskytovatelé informačních a komunikačních služeb měli přímý vztah s jednotlivci v EU (na základě nabídky on-line služeb), mohlo by to vést k přímému použití nařízení (EU) 2016/679 podle jeho čl. 3 odst. 2 písm. a).

([39]) Ustanovení čl. 58 odst. 2 zákona o ochraně osobních údajů dále stanoví, že články 15 a 22, čl. 27 odst. 1 a 2 a články 34 a 37 se nepoužijí na osobní údaje zpracovávané pomocí zařízení pro vizuální zpracování dat instalovaných a provozovaných na veřejně přístupných místech. Jelikož se toto ustanovení týká používání kamerového dohledu v Koreji, tj. přímého shromažďování osobních údajů od jednotlivců v Koreji, není relevantní pro účely tohoto rozhodnutí, které se týká předávání osobních údajů od správců/zpracovatelů v EU subjektům v Koreji. Kromě toho se podle čl. 58 odst. 3 zákona o ochraně osobních údajů článek 15 (shromažďování a používání osobních údajů), článek 30 (povinnost zavést zásady ochrany soukromí) a článek 31 (povinnost jmenovat pověřence pro ochranu soukromí) nepoužijí na osobní údaje, které jsou zpracovávány za účelem provozování neformálních volnočasových skupin nebo sdružení (např. zájmové kluby). Má se za to, že tyto skupiny mají osobní povahu a nemají žádnou spojitost s profesionální nebo obchodní činností, a tudíž není pro shromažďování a používání jejich informací v této souvislosti vyžadován žádný konkrétní právní základ (například souhlas dotčených osob). Všechna ostatní ustanovení zákona o ochraně osobních údajů (např. minimalizace údajů, účelové omezení, zákonnost zpracování, zabezpečení a individuální práva) jsou však nadále použitelná. Kromě toho by výjimku nebylo možné využít pro jakékoli zpracování osobních údajů nad rámec účelu spočívajícího ve vytvoření společenské skupiny.

([40]) Konkrétně čl. 58 odst. 4 zákona o ochraně osobních údajů stanoví povinnost zpracovávat osobní údaje v minimálním rozsahu nezbytném pro dosažení zamýšleného účelu, zpracovávat je po minimální dobu a přijmout nezbytná opatření pro bezpečnou správu a náležité zpracování takových osobních údajů. Nezbytná opatření zahrnují technické, řídicí a fyzické záruky, jakož i opatření k zajištění řádného vyřízení jednotlivých stížností.

(27) Zaprvé se dílčí výjimka vztahuje na osobní údaje shromážděné podle zákona o statistice pro účely zpracování veřejnými institucemi. Podle objasnění obdržených od korejské vlády se osobní údaje zpracovávané v této souvislosti obvykle týkají korejských státních příslušníků a pouze výjimečně mohou zahrnovat údaje o cizích státních příslušnících, a to v případě statistických údajů o vstupu na území a opuštění území nebo o zahraničních investicích. I v těchto situacích však tyto údaje obvykle nejsou předávány správcem/zpracovatelem v Unii, ale spíše je přímo shromažďují orgány veřejné správy v Koreji ([41]). Kromě toho zákon o statistice – podobně jako stanoví 162. bod odůvodnění nařízení (EU) 2016/679 – také ukládá pro zpracování údajů několik podmínek a záruk. Zejména ukládá specifické povinnosti, jako je zajistit přesnost, konzistentnost a nestrannost, zaručit utajení fyzických osob, chránit údaje respondentů v souvislosti se statistickými dotazy, a to mimo jiné s cílem zabránit tomu, aby byly tyto údaje použity k jakémukoli jinému účelu než pro sestavování statistik, a uložit zaměstnancům povinnost dodržet požadavky v oblasti důvěrnosti ([42]). Orgány veřejné správy, které zpracovávají statistiky, musí rovněž dodržovat mimo jiné zásady minimalizace údajů, účelového omezení a zabezpečení údajů (článek 3 a čl. 58 odst. 4 zákona o ochraně osobních údajů) a umožnit jednotlivcům výkon jejich práv (na přístup, opravu, výmaz a pozastavení zpracování, viz článek 4 zákona o ochraně osobních údajů). A konečně, osobní údaje musí být zpracovávány v anonymizované nebo pseudonymizované podobě, pokud to umožňuje naplnit účel zpracování (čl. 3 odst. 7 zákona o ochraně osobních údajů).

(28) Zadruhé čl. 58 odst. 1 zákona o ochraně osobních údajů zmiňuje osobní údaje shromážděné nebo požadované pro analýzu informací souvisejících s národní bezpečností. Oblast působnosti a důsledky této dílčí výjimky jsou podrobněji popsány ve 149. bodě odůvodnění.

(29) Zatřetí se dílčí výjimka vztahuje na dočasné zpracování osobních údajů, pokud je toto zpracování naléhavě nutné z důvodů veřejné bezpečnosti či ochrany, včetně veřejného zdraví. Komise pro ochranu osobních údajů vykládá tuto kategorii striktně a podle informací obdržených od korejské vlády ji nikdy nepoužila. Tato kategorie se vztahuje pouze na mimořádné události vyžadující naléhavá opatření, například sledování infekčních činitelů nebo záchranu obětí přírodních katastrof a pomoc těmto obětem ([43]). Dokonce i v těchto situacích se dílčí výjimka vztahuje pouze na zpracování osobních údajů po omezenou dobu za účelem provedení takového opatření. Situace, kdy by se tato výjimka mohla týkat předávání údajů, na něž se vztahuje toto rozhodnutí, jsou ještě omezenější, vzhledem k nízké pravděpodobnosti toho, že by osobní údaje předávané z Unie korejským hospodářským subjektům byly takového druhu, že by jejich následné zpracování bylo pro takové mimořádné situace „naléhavě nezbytné“.

(30) A konečně se dílčí výjimka použije na osobní údaje shromážděné nebo použité tiskem, pro misijní činnosti náboženských organizací nebo nominace kandidátů politickými stranami. Výjimka se použije pouze v případech, kdy jsou osobní údaje zpracovávány tiskem, náboženskými organizacemi nebo politickými stranami pro tyto konkrétní účely (tj. novinářská činnost, misijní práce a nominace politických kandidátů). Pokud tyto subjekty zpracovávají osobní údaje pro jiné účely, například pro řízení lidských zdrojů nebo vnitřní administrativu, použije se zákon o ochraně osobních údajů v plném rozsahu.

(31) Pokud jde o zpracování osobních údajů tiskem pro novinářskou činnost, je vyvážení svobody projevu a dalších práv (včetně práva na soukromí) stanoveno zákonem o rozhodčím řízení a opravných prostředcích apod. ve věci škody způsobené tiskovými zprávami (dále jen „tiskový zákon“) ([44]). Konkrétně článek 5 tiskového zákona

([41]) V tomto ohledu článek 33 zákona o statistice požaduje, aby veřejné instituce chránily údaje respondentů v souvislosti se statistickými dotazy, mimo jiné s cílem zabránit tomu, aby tyto údaje byly použity k jinému účelu než k sestavování statistik.
([42]) Ustanovení čl. 2 odst. 2 a 3, čl. 30 odst. 2 a článků 33 a 34 zákona o statistice.
([43]) Příručka k zákonu o ochraně osobních údajů, oddíl týkající se článku 58.
([44]) Například článek 4 tiskového zákona stanoví, že tiskové zprávy musí být nestranné a objektivní, ve veřejném zájmu, musí respektovat lidskou důstojnost a hodnotu a nesmí hanobit jiné osoby ani porušovat jejich práva, veřejnou morálku nebo společenskou etiku.

stanoví, že tisk (tj. jakákoli vysílací organizace, denní tisk, periodikum nebo on-line noviny) ani jakákoli internetová zpravodajská služba nebo internetová multimediální vysílací organizace nesmí narušovat soukromí jednotlivců. Pokud přesto dojde k narušení soukromí, musí být neprodleně napraveno v souladu s konkrétními postupy stanovenými v zákoně. V tomto ohledu zákon přiznává jednotlivcům, kteří utrpí újmu v důsledku tiskové zprávy, řadu práv, například právo dosáhnout zveřejnění opravy nepravdivého prohlášení, opravy prostřednictvím protichůdného prohlášení nebo další zprávy (pokud se tisková zpráva týká obvinění z trestných činů, kterých je jednotlivec později zproštěn) ([45]). Nároky jednotlivců mohou být řešeny přímo tiskovými subjekty (prostřednictvím veřejného ochránce práv) ([46]), prostřednictvím smírčího nebo rozhodčího řízení (před specializovanou rozhodčí komisí pro tisk) ([47]) nebo u soudu. Jednotlivci mohou také získat odškodnění, pokud utrpí peněžní újmu, narušení osobnostního práva nebo jakoukoli jinou emocionální újmu v důsledku nezákonného jednání tisku (úmyslného nebo nedbalostního) ([48]). Tisk je zproštěn odpovědnosti podle zákona v rozsahu, v jakém tisková zpráva, která zasahuje do práv jednotlivce, není v rozporu se společenskými hodnotami a je zveřejněna buď se souhlasem dotčené osoby, nebo ve veřejném zájmu (a existují dostatečné důvody k domněnce, že zpráva odpovídá pravdě) ([49]).

(32) Zatímco zpracování osobních údajů tiskem pro účely novinářské činnosti podléhá zvláštním zárukám, které vyplývají z tiskového zákona, neexistují žádná taková další opatření, která by vymezovala použití výjimek pro činnosti zpracování náboženskými organizacemi a politickými stranami způsobem srovnatelným s články 85, 89 a 91 nařízení (EU) 2016/679. Komise proto považuje za vhodné vyloučit z oblasti působnosti tohoto rozhodnutí náboženské organizace, pokud zpracovávají osobní údaje pro svou misijní činnost, a politické strany, pokud zpracovávají osobní údaje v souvislosti s nominací kandidátů.

2.3 **Záruky, práva a povinnosti**

2.3.1 *Zákonnost a korektnost zpracování*

(33) Osobní údaje by měly být zpracovávány zákonným a korektním způsobem.

(34) Tato zásada je stanovena v čl. 3 odst. 1 a 2 zákona o ochraně osobních údajů a posílena článkem 59 zákona o ochraně osobních údajů, který zakazuje zpracování osobních údajů „podvodem, nevhodnými nebo nekalými prostředky“, „bez zákonného oprávnění“ nebo „nad rámec řádného oprávnění“ ([50]). Tyto obecné zásady zákonného zpracování jsou rozpracovány v článcích 15 až 19 zákona o ochraně osobních údajů, které stanoví různé právní základy pro zpracování (shromažďování, používání a poskytování třetím stranám), včetně okolností, za kterých tato činnost může zahrnovat změnu účelu (článek 18 zákona o ochraně osobních údajů).

([45]) Články 15 až 17 tiskového zákona.

([46]) Každý tiskový nebo mediální subjekt musí mít vlastního veřejného ochránce práv, aby zabránil případným škodám způsobeným tiskem nebo takové škody napravil (např. doporučením opravy tiskových zpráv, které jsou nepravdivé nebo poškozují pověst jiných osob), článek 6 tiskového zákona.

([47]) Komisi tvoří 40 až 90 rozhodců jmenovaných ministrem kultury, sportu a cestovního ruchu z řad osob s kvalifikací soudců, advokátů, osob zabývajících se shromažďováním nebo vydáváním zpráv po dobu nejméně deseti let nebo jiných osob s odborností související s tiskem. Rozhodci nemohou být zároveň veřejnými činiteli, členy politických stran nebo novináři. V souladu s článkem 8 tiskového zákona musí rozhodci vykonávat své povinnosti nezávisle a nesmí v souvislosti s těmito povinnostmi podléhat žádným pokynům nebo instrukcím. Kromě toho jsou zavedena zvláštní pravidla, která zabraňují střetu zájmů, např. vyloučením jednotlivých rozhodců z projednávání jednotlivých případů, pokud jsou účastníky v dané věci jejich manžel/ka nebo příbuzní (článek 10 tiskového zákona). Komise může spory řešit smírčím nebo rozhodčím řízením, může však také vydat doporučení k nápravě porušení (článek 5 tiskového zákona).

([48]) Článek 30 tiskového zákona.

([49]) Článek 5 tiskového zákona.

([50]) Článek 59 zákona o ochraně osobních údajů zakazuje jakékoli osobě, „která zpracovává nebo někdy zpracovávala osobní údaje“, „získat osobní údaje nebo souhlas se zpracováním osobních údajů podvodem, nevhodnými nebo nekalými prostředky“, „vyzradit osobní údaje získané v rámci podnikání nebo je poskytnout kterékoli třetí straně bez oprávnění“ nebo „poškodit, zničit, pozměnit, padělat nebo vyzradit osobní údaje jiných osob bez zákonného oprávnění nebo nad rámec řádného oprávnění“. Porušení tohoto zákazu může vést k trestním sankcím, viz čl. 71 odst. 5 a 6 a čl. 72 odst. 2 zákona o ochraně osobních údajů. Ustanovení čl. 70 odst. 2 zákona o ochraně osobních údajů dále umožňuje uložit trestní sankci za získávání osobních údajů zpracovávaných třetími stranami podvodem nebo jinými nekalými prostředky nebo metodami nebo za poskytnutí takových údajů třetí straně za účelem dosažení zisku nebo za nekalým účelem, jakož i za navádění k takovému jednání nebo organizování takového jednání.

(35) Podle čl. 15 odst. 1 zákona o ochraně osobních údajů může správce shromažďovat osobní údaje (v rozsahu účelu shromažďování) pouze z omezeného počtu právních důvodů. Těmito důvody jsou 1) souhlas subjektu údajů ([51]) (bod 1); 2) nezbytnost uzavřít a plnit smlouvu se subjektem údajů (bod 4); 3) zvláštní oprávnění na základě zákona nebo nezbytnost pro splnění zákonné povinnosti (bod 2); případ, kdy je nezbytné ([52]), aby veřejná instituce v rámci své jurisdikce vykonávala úkoly předepsané zákonem; 4) zjevná nezbytnost ochrany života, zdraví nebo majetkových zájmů subjektu údajů nebo třetí strany před bezprostředním nebezpečím (pouze pokud subjekt údajů není schopen vyjádřit svůj úmysl nebo nelze získat souhlas předem) (bod 5); 5) nezbytnost dosáhnout „oprávněného zájmu“ správce, pokud je „zjevně nadřazen“ zájmům subjektu údajů (a pouze v případě, že zpracování má „podstatný vztah“ k oprávněnému zájmu a nepřekračuje rámec přiměřenosti) (bod 6) ([53]). Tyto důvody pro zpracování jsou v zásadě rovnocenné důvodům stanoveným v článku 6 nařízení (EU) 2016/679, včetně důvodu „oprávněného zájmu“, který je rovnocenný důvodu „oprávněného zájmu“ podle čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679.

(36) Jakmile jsou osobní údaje shromážděny, mohou být použity v rámci účelu shromažďování (čl. 15 odst. 1 zákona o ochraně osobních údajů) nebo „v rozsahu přiměřeně souvisejícím“ s účelem shromažďování, s přihlédnutím k možným znevýhodněním způsobeným subjektu údajů a za předpokladu, že jsou přijata nezbytná bezpečnostní opatření (např. šifrování) (čl. 15 odst. 3 zákona o ochraně osobních údajů). Pro určení toho, zda účel použití „přiměřeně souvisí“ s původním účelem shromažďování, stanoví prováděcí vyhláška zvláštní kritéria, která jsou obdobná těm, jež jsou uvedena v čl. 6 odst. 4 nařízení (EU) 2016/679. Zejména musí existovat značná relevance ve vztahu k původnímu účelu; dodatečné použití musí být předvídatelné (například s ohledem na okolnosti, za nichž byly údaje shromážděny); a pokud je to možné, údaje musí být pseudonymizovány ([54]). Zvláštní kritéria použitá správcem při tomto posouzení musí být předem zveřejněna v zásadách ochrany soukromí ([55]). Kromě toho je pověřenec pro ochranu soukromí údajů (viz 94. bod odůvodnění) výslovně povinen přezkoumat, zda v rámci těchto parametrů dochází k dalšímu použití.

([51]) Souhlas musí být poskytnut svobodně, informovaně, konkrétně a musí být vyjádřen jedním z několika způsobů určených zákonem. V žádném případě nelze souhlas získat podvodem, nevhodnými nebo jinak nekalými prostředky (čl. 59 odst. 1 zákona o ochraně osobních údajů). Zaprvé mají podle čl. 4 bodu 2 zákona o ochraně osobních údajů subjekty údajů právo „souhlasit nebo nesouhlasit“ a „zvolit rozsah souhlasu“ a měly by být o tom informovány (čl. 15 odst. 2, čl. 16 odst. 2 a 3, čl. 17 odst. 2 a 18 odst. 3 zákona o ochraně osobních údajů). Ustanovení čl. 22 odst. 5 zákona o ochraně osobních údajů obsahuje další záruku, neboť zakazuje správci odmítnout poskytování zboží nebo služeb, pokud by to mohlo ohrozit svobodné rozhodování jednotlivce při udělení souhlasu. To zahrnuje situace, kdy souhlas vyžadují pouze určité druhy zpracování (zatímco jiné jsou založeny na smlouvě), a také další zpracování osobních údajů shromážděných v souvislosti s poskytováním zboží nebo služeb. Zadruhé musí podle čl. 15 odst. 2, čl. 17 odst. 2 a 3 a čl. 18 odst. 3 zákona o ochraně osobních údajů správce při žádosti o souhlas sdělit subjektu údajů „podrobnosti“ dotčených osobních údajů (např. že jde o citlivé údaje, viz čl. 17 odst. 2 bod 2 písm. a) prováděcí vyhlášky k zákonu o ochraně osobních údajů), účel zpracování, dobu uchovávání a všechny příjemce údajů. Každá taková žádost musí být podána „výslovně rozpoznatelným způsobem“, který odlišuje záležitosti vyžadující souhlas od jiných záležitostí (čl. 22 odst. 1 až 4 zákona o ochraně osobních údajů). Zatřetí čl. 17 odst. 1 body 1 až 6 prováděcí vyhlášky k zákonu o ochraně osobních údajů stanoví konkrétní metody, kterými správce získá souhlas, například písemný souhlas s podpisem subjektu údajů nebo souhlas elektronickou poštou (odpovědí na e-mail). Zákon o ochraně osobních údajů sice výslovně neposkytuje fyzickým osobám obecné právo odvolat souhlas, ale tyto osoby mají právo dosáhnout pozastavení zpracování údajů, které se jich týkají, přičemž uplatnění tohoto práva vede k ukončení zpracování údajů a k jejich výmazu (viz 78. bod odůvodnění týkající se práva na pozastavení zpracování).

([52]) Podle informací obdržených od Komise pro ochranu osobních údajů mohou veřejné instituce tohoto důvodu využít pouze tehdy, je-li zpracování osobních údajů nevyhnutelné, tj. musí být nemožné nebo nepřiměřeně obtížné, aby instituce vykonávala své funkce bez zpracování údajů.

([53]) Článek 39-3 zákona o ochraně osobních údajů ukládá poskytovatelům informačních a komunikačních služeb specifické (přísnější) povinnosti, pokud jde o shromažďování a používání osobních údajů jejich uživatelů. Zejména vyžaduje, aby poskytovatel získal souhlas uživatele poté, co poskytne informace o účelu shromažďování/použití, kategoriích osobních údajů, které mají být shromažďovány, a o době, po kterou budou údaje zpracovávány (čl. 39-3 odst. 1 zákona o ochraně osobních údajů). Totéž platí při změně kteréhokoli z těchto aspektů. Nezískání souhlasu se shromažďováním údajů podléhá trestním sankcím (čl. 71 body 4 a 5 zákona o ochraně osobních údajů. Výjimečně mohou poskytovatelé informačních a komunikačních služeb shromažďovat nebo používat osobní údaje uživatelů bez předchozího souhlasu. Je tomu tak v případě, že 1) je zjevně obtížné získat běžný souhlas pro osobní údaje potřebné k plnění smlouvy upravující poskytování informačních a komunikačních služeb z hospodářských a technologických důvodů (např. pokud během procesu plnění smlouvy nevyhnutelně vznikají osobní údaje, jako jsou fakturační údaje, přístupové protokoly a záznamy o platbách); 2) je to nezbytné pro úhradu poplatků po poskytování informačních a komunikačních služeb, nebo 3) umožňují-li to jiné zákony (např. čl. 21 odst. 1 bod 6 zákona o ochraně spotřebitele v rámci elektronického obchodování stanoví, že podnikatelské subjekty mohou shromažďovat osobní údaje o zákonných zástupcích nezletilé osoby za účelem potvrzení toho, že byl získán platný souhlas jménem nezletilé osoby) (čl. 39-3 odst. 2 zákona o ochraně osobních údajů). Ve všech případech nesmí poskytovatelé informačních a komunikačních služeb odmítnout poskytování služeb jen z toho důvodu, že uživatel neposkytne více osobních údajů, než je požadované minimum (tj. údaje, které jsou nezbytné k realizaci základních prvků dotčené služby), viz čl. 39-3 odst. 3 zákona o ochraně osobních údajů.

([54]) Viz článek 14-2 prováděcí vyhlášky k zákonu o ochraně osobních údajů.

([55]) Ustanovení čl. 14-2 odst. 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů.

(37) Podobná (avšak poněkud přísnější) pravidla platí pro poskytování údajů třetí straně. Podle čl. 17 odst. 1 zákona o ochraně osobních údajů je poskytnutí osobních údajů třetí straně povoleno na základě souhlasu ([56]) nebo v rámci účelu shromažďování, pokud byly údaje shromážděny z jednoho z právních důvodů podle čl. 15 odst. 1 bodů 2, 3 a 5 zákona o ochraně osobních údajů. To vylučuje zejména jakékoli zpřístupnění založené na „oprávněném zájmu“ správce. Kromě toho čl. 17 odst. 4 zákona o ochraně osobních údajů umožňuje poskytnutí třetí straně „v rozsahu přiměřeně souvisejícím“ s účelem shromažďování, opět s přihlédnutím k možným znevýhodněním způsobeným subjektu údajů a za předpokladu, že jsou přijata nezbytná bezpečnostní opatření (např. šifrování). Stejné faktory, jaké jsou popsány v 36. bodě odůvodnění, je třeba vzít v úvahu při posouzení toho, zda poskytnutí spadá do oblasti přiměřeně související s účelem shromažďování a zda se použijí stejné záruky (tj. s ohledem na transparentnost prostřednictvím zásad ochrany soukromí a zapojení pověřence pro ochranu soukromí).

(38) Přijetí osobních údajů z Unie korejským správcem údajů se považuje za „shromažďování“ ve smyslu článku 15 zákona o ochraně osobních údajů. Oznámení č. 2021-5 (oddíl I přílohy I tohoto rozhodnutí) objasňuje, že účel, pro který byly údaje předány dotčeným subjektem v EU, představuje účel shromažďování údajů pro korejského správce údajů. V důsledku toho jsou korejští správci údajů, kteří přijímají osobní údaje z Unie, v zásadě povinni zpracovávat tyto údaje v rámci účelu předání v souladu s článkem 17 zákona o ochraně osobních údajů.

(39) Zvláštní omezení platí v případě, že správce hodlá použít osobní údaje nebo je poskytnout třetí straně k účelu jinému, než je účel shromažďování ([57]). Podle čl. 18 odst. 2 zákona o ochraně osobních údajů může soukromý správce výjimečně ([58]) použít osobní údaje nebo je poskytnout třetí straně k jinému účelu: 1) na základě dodatečného (tedy samostatného) souhlasu subjektu údajů; 2) stanoví-li to zvláštní zákonná ustanovení, nebo 3) je-li to zjevně nezbytné k ochraně života, zdraví nebo majetkových zájmů subjektu údajů nebo třetí strany před bezprostředním nebezpečím (pouze pokud subjekt údajů není schopen vyjádřit svůj úmysl nebo nelze získat souhlas předem) ([59]).

(40) Veřejné instituce mohou v určitých situacích používat osobní údaje nebo je poskytovat třetí straně také k jinému účelu. To zahrnuje případy, kdy by jinak nebylo možné, aby veřejné instituce vykonávaly své zákonné povinnosti předepsané právními předpisy, s výhradou povolení Komise pro ochranu osobních údajů. Kromě toho mohou veřejné instituce poskytnout osobní údaje jinému orgánu nebo soudu, je-li to nezbytné pro vyšetřování a trestní stíhání trestných činů nebo pro podání obžaloby, k tomu, aby soud vykonával své funkce související s probíhajícím soudním řízením, nebo k výkonu trestu nebo soudního příkazu k zajištění péče nebo vazby ([60]). Mohou také poskytnout osobní údaje zahraniční vládě nebo mezinárodní organizaci, aby splnily zákonnou povinnost vyplývající ze smlouvy nebo mezinárodní úmluvy, přičemž v takovém případě musí rovněž splnit požadavky na přeshraniční předávání údajů (viz 90. bod odůvodnění).

(41) Zásady zákonnosti a korektnosti zpracování jsou proto v korejském právním rámci provedeny v zásadě rovnocenným způsobem jako v nařízení (EU) 2016/679, neboť zpracování je povoleno pouze na základě legitimních a jasně definovaných důvodů. Kromě toho je ve všech uvedených případech zpracování povoleno pouze tehdy, pokud není pravděpodobné, že by „nekorektním způsobem narušilo“ zájmy subjektu údajů nebo třetí strany, což vyžaduje vyvážení zájmů. Kromě toho čl. 18 odst. 5 zákona o ochraně osobních údajů předepisuje další záruky, pokud správce poskytne osobní údaje třetí straně, a ty mohou zahrnovat požadavek na omezení účelu a způsobu použití nebo na zavedení zvláštních bezpečnostních opatření. Třetí strana je pak povinna požadovaná opatření provést.

([56]) Porušení čl. 17 odst. 1 bodu 1 zákona o ochraně osobních údajů může vést k uložení trestních sankcí (čl. 71 odst. 1 zákona o ochraně osobních údajů).

([57]) „Zamýšlený účel“ je účel, pro který byly údaje shromážděny. Pokud jsou například údaje shromažďovány na základě souhlasu dotčené fyzické osoby, zamýšleným účelem je účel, který je této fyzické osobě sdělen podle čl. 15 odst. 2 zákona o ochraně osobních údajů.

([58]) Srov. čl. 18 odst. 1 zákona o ochraně osobních údajů. Porušení čl. 18 odst. 1 a 2 může vést k uložení trestních sankcí (čl. 71 odst. 2 zákona o ochraně osobních údajů).

([59]) Použití osobních údajů nebo jejich poskytnutí třetí straně poskytovateli informačních a komunikačních služeb za jiným než původním účelem může být provedeno pouze z důvodů uvedených v čl. 18 odst. 2 bodě 1 a 2 zákona o ochraně osobních údajů (tj. je-li získán dodatečný souhlas nebo existují-li zvláštní zákonná ustanovení). Viz čl. 18 odst. 2 zákona o ochraně osobních údajů.

([60]) S výjimkou případů, kdy je zpracování nezbytné pro vyšetřování a trestných činů, podání obžaloby a trestní stíhání, jsou veřejné instituce, které používají osobní údaje nebo je poskytují třetí straně za jiným účelem, než za jakým byly shromážděny (například pokud to zákon výslovně povoluje nebo je-li to nezbytné k plnění úmluvy), povinny zveřejnit na svých internetových stránkách nebo v úředním věstníku právní důvody zpracování, jeho účel a rozsah a vést záznamy (čl. 18 odst. 4 zákona o ochraně osobních údajů ve spojení s článkem 15 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

(42) A konečně článek 28-2 zákona o ochraně osobních údajů umožňuje (další) zpracování pseudonymizovaných údajů bez souhlasu dotčené osoby pro účely statistiky, vědeckého výzkumu ([61]) a archivace ve veřejném zájmu, s výhradou zvláštních záruk. Obdobně jako nařízení (EU) 2016/679 ([62]) proto zákon o ochraně osobních údajů usnadňuje (další) zpracování osobních údajů pro takové účely v rámci, který stanoví vhodné záruky na ochranu práv jednotlivců. Namísto toho, aby zákon o ochraně osobních údajů uplatňoval pseudonymizaci jako možnou záruku, ukládá ji jako podmínku pro provádění určitých činností zpracování pro účely statistiky, vědeckého výzkumu a archivace ve veřejném zájmu (například aby bylo možné zpracovávat údaje bez souhlasu nebo kombinovat různé datové soubory).

(43) Zákon o ochraně osobních údajů navíc ukládá řadu zvláštních záruk, zejména pokud jde o požadovaná technická a organizační opatření, vedení záznamů, omezení sdílení údajů a řešení možných rizik opětovné identifikace. Kombinace jednotlivých záruk popsaných ve 44. až 48. bodě odůvodnění zajišťuje, že zpracování osobních údajů v této souvislosti podléhá v zásadě rovnocenné ochraně ve srovnání s ochranou, která by byla vyžadována podle nařízení (EU) 2016/679.

(44) Zaprvé a především čl. 28-5 odst. 1 zákona o ochraně osobních údajů zakazuje zpracování pseudonymizovaných údajů za účelem identifikace určité osoby. Pokud by přesto při zpracování pseudonymizovaných údajů vznikly údaje, které by mohly určitou fyzickou osobu identifikovat, musí správce okamžitě pozastavit zpracování a tyto údaje zničit (čl. 28-5 odst. 2 zákona o ochraně osobních údajů). Nedodržení těchto ustanovení podléhá správním pokutám a představuje trestný čin ([63]). To znamená, že i v situacích, kdy by bylo *prakticky* možné danou osobu opětovně identifikovat, je takováto opětovná identifikace *ze zákona* zakázána.

(45) Zadruhé musí správce při (dalším) zpracování pseudonymizovaných údajů pro tyto účely zavést zvláštní technická, řídicí a fyzická opatření k zajištění bezpečnosti údajů (včetně samostatného ukládání a správy údajů nezbytných k uvedení pseudonymizovaných údajů do původního stavu) ([64]). Kromě toho musí vedeny záznamy o zpracovávaných pseudonymizovaných údajích, účelu zpracování, historii použití a případných přijímajících třetích stranách (článek 29-5 odst. 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

(46) A konečně zatřetí zákon o ochraně osobních údajů stanoví zvláštní záruky, které mají zabránit identifikaci fyzických osob třetími stranami v případě sdílení údajů. Konkrétně při poskytování pseudonymizovaných údajů třetí straně za účelem statistiky, vědeckého výzkumu nebo archivace ve veřejném zájmu nesmí správci zahrnout údaje, které by mohly být použity k identifikaci konkrétní fyzické osoby (čl. 28-2 odst. 2 zákona o ochraně osobních údajů) ([65]).

(47) Přesněji řečeno, ačkoli zákon o ochraně osobních údajů umožňuje kombinaci pseudonymizovaných údajů (zpracovávaných různými správci) pro účely statistiky, vědeckého výzkumu nebo archivace ve veřejném zájmu, vyhrazuje tuto pravomoc specializovaným institucím vybaveným konkrétními bezpečnostními zařízeními (článek 28-3 odst. 1) zákona o ochraně osobních údajů) ([66]). Při žádosti o kombinaci pseudonymizovaných údajů musí správce předložit dokumenty, které mimo jiné uvádí údaje, jež mají být zkombinovány, účel kombinace, jakož

([61]) Vědecký výzkum je v čl. 2 odst. 8 zákona o ochraně osobních údajů definován jako „výzkum, který využívá vědecké metody, jako jsou technologický vývoj a technologické demonstrace, základní výzkum, aplikovaný výzkum a výzkum financovaný ze soukromých zdrojů“. Tyto kategorie odpovídají kategoriím vymezeným ve 159. bodě odůvodnění nařízení (EU) 2016/679.

([62]) Viz čl. 5 odst. 1 písm. b) a čl. 89 odst. 1 a 2 a 50. a 157. bod odůvodnění nařízení (EU) 2016/679.

([63]) Viz čl. 28-6 odst. 1, čl. 71 odst. 4-3 a čl. 75 odst. 2 bod 4-4 zákona o ochraně osobních údajů.

([64]) Článek 28-4 zákona o ochraně osobních údajů a článek 29-5 prováděcí vyhlášky k zákonu o ochraně osobních údajů. Nesplnění této povinnosti podléhá správním a trestním sankcím, viz čl. 73 odst. 1 a čl. 75 odst. 2 bod 6 zákona o ochraně osobních údajů.

([65]) Porušení těchto požadavků může vést k uložení trestních sankcí (čl. 71 odst. 2 zákona o ochraně osobních údajů). Komise pro ochranu osobních údajů začala okamžitě tato nová pravidla prosazovat, např. v rozhodnutí ze dne 28. dubna 2021, kterým uložila pokutu a nápravná opatření společnosti, která mimo jiná porušení zákona o ochraně osobních údajů nesplnila požadavek uvedený v čl. 28-2 odst. 2 tohoto zákona, viz https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([66]) Aby byla instituce jmenována takovou specializovanou institucí („odborná agentura pro kombinaci údajů“), musí být Komisi pro ochranu osobních údajů podána žádost spolu s podpůrnou dokumentací, která mimo jiné podrobně popisuje zařízení a vybavení zavedené pro bezpečné kombinování pseudonymizovaných údajů a potvrzuje, že žadatel zaměstnává nejméně tři zaměstnance na plný úvazek s kvalifikací nebo praxí v oblasti ochrany osobních údajů (čl. 29-2 odst. 1 a 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů). Podrobné požadavky, např. na kvalifikaci personálu, dostupná zařízení, bezpečnostní opatření, vnitřní zásady a postupy, jakož i finanční požadavky jsou uvedeny v oznámení Komise pro ochranu osobních údajů č. 2020-9 o kombinaci a uvolňování pseudonymizovaných údajů (příloha I). Jmenování odbornou agenturou pro kombinaci údajů může Komise pro ochranu osobních údajů (po slyšení) z určitých důvodů zrušit, např. pokud agentura již nesplňuje bezpečnostní standardy požadované pro jmenování nebo pokud v souvislosti s kombinací údajů došlo k narušení zabezpečení údajů (čl. 29-2 odst. 5 a 6 prováděcí vyhlášky k zákonu o ochraně osobních údajů). Komise pro ochranu osobních údajů musí zveřejnit každé jmenování (nebo zrušení jmenování) odborné agentury pro kombinaci údajů (čl. 29-2 odst. 7 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

i navrhovaná bezpečnostní opatření pro zpracování kombinovaných údajů ([67]). Aby bylo možné kombinování provést, musí správce odeslat údaje, které mají být zkombinovány, specializované instituci a poskytnout „kombinační klíč“ (tj. údaje, které byly použity pro pseudonymizaci) Korejské agentuře pro internet a zabezpečení ([68]). Ta vygeneruje „propojovací údaje kombinačního klíče“ (které umožní propojit kombinační klíče různých žadatelů za účelem dosažení kombinace datových souborů) a poskytne je specializované instituci ([69]).

(48) Správce, který žádá o kombinaci, může zkombinované údaje analyzovat v budově specializované instituce, v prostoru, kde jsou zavedena zvláštní technická, fyzická a administrativní bezpečnostní opatření (článek 29-3 prováděcí vyhlášky k zákonu o ochraně osobních údajů). Správci, kteří k takové kombinaci přispějí datovým souborem, mohou zkombinované údaje přenést mimo specializovanou instituci až po další pseudonymizaci nebo anonymizaci zkombinovaných údajů a se souhlasem této instituce (čl. 28-3 odst. 2 zákona o ochraně osobních údajů) ([70]). Při posuzování toho, zda takový souhlas udělit či nikoli, posoudí instituce souvislost mezi zkombinovanými údaji a účelem zpracování a to, zda byl pro použití těchto údajů vypracován zvláštní bezpečnostní plán ([71]). Export zkombinovaných údajů mimo instituci nebude povolen, pokud údaje obsahují informace, které by umožnily identifikaci určité fyzické osoby ([72]). A konečně také na kombinování a uvolňování pseudonymizovaných údajů specializovanou institucí dohlíží Komise pro ochranu osobních údajů (čl. 29-4 odst. 3 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

2.3.2 *Zpracování zvláštních kategorií osobních údajů*

(49) Pokud se zpracovávají „zvláštní kategorie“ údajů, měly by existovat zvláštní záruky.

(50) Zákon o ochraně osobních údajů obsahuje zvláštní pravidla pro zpracování citlivých údajů ([73]), které jsou definovány jako osobní údaje odhalující údaje o ideologii, přesvědčení, přijetí do odborové organizace nebo politické strany nebo vystoupení z ní, o politických názorech, zdraví a sexuálním životě jednotlivce, jakož i další osobní údaje, které by mohly „zjevně“ ohrozit soukromí subjektu údajů a v prezidentské vyhlášce jsou označeny jako citlivé údaje ([74]). Podle vysvětlení získaných od Komise pro ochranu osobních údajů je sexuální život vykládán tak, že zahrnuje i sexuální orientaci nebo preference jednotlivce ([75]). Kromě toho článek 18 prováděcí vyhlášky doplňuje rozsah citlivých údajů o další kategorie, zejména údaje o DNA získané genetickým testováním a údaje, které představují záznam v trestním rejstříku. Nedávná novela prováděcí vyhlášky k zákonu o ochraně osobních údajů dále rozšířila pojem citlivých údajů tím, že zahrnula také osobní údaje odhalující rasový nebo etnický původ a biometrické údaje ([76]). Po této novele je pojem citlivých údajů podle zákona o ochraně osobních údajů v zásadě rovnocenný pojmu uvedenému v článku 9 nařízení (EU) 2016/679.

(51) Podle čl. 23 odst. 1 zákona o ochraně osobních údajů a obdobně jako podle čl. 9 odst. 1 nařízení (EU) 2016/679 je zpracování citlivých údajů obecně zakázáno, pokud se nepoužije některá z vyjmenovaných výjimek ([77]). Tyto výjimky omezují zpracování na případy, kdy správce informuje subjekt údajů v souladu s články

([67]) Ustanovení čl. 8 odst. 1 a 2 oznámení č. 2020-9 o kombinaci a uvolňování pseudonymizovaných údajů.
([68]) Ustanovení čl. 2 odst. 3 a 6 a čl. 9 odst. 1 oznámení č. 2020-9 o kombinaci a uvolňování pseudonymizovaných údajů.
([69]) Ustanovení čl. 2 odst. 4 a čl. 9 odst. 2 a 3 oznámení č. 2020-9 o kombinaci a uvolňování pseudonymizovaných údajů. Specializovaná instituce musí propojovací údaje kombinačního klíče po spojení okamžitě zničit (čl. 9 odst. 4 oznámení).
([70]) Porušení požadavků týkajících se kombinace datových souborů může vést k uložení trestních sankcí (čl. 71 bod 4-2 zákona o ochraně osobních údajů). Viz také čl. 29-2 odst. 4 prováděcí vyhlášky k zákonu o ochraně osobních údajů.
([71]) Postup pro schvalování uvolnění zkombinovaných údajů je stanoven v článku 11 oznámení č. 2020-9 o kombinaci a uvolňování pseudonymizovaných údajů. Specializovaná instituce musí zejména zřídit „výbor pro přezkum uvolnění“ složený ze členů s náležitými znalostmi a praxí v oblasti ochrany údajů.
([72]) Ustanovení čl. 29-2 odst. 4 prováděcí vyhlášky k zákonu o ochraně osobních údajů a článek 11 oznámení č. 2020-9.
([73]) Nutnost poskytnout zvláštní ochranu zpracování citlivých údajů, jako jsou údaje týkající se zdraví nebo sexuálního chování, uznal také korejský Ústavní soud, viz rozhodnutí Ústavního soudu HunMa 1139, 31. května 2007.
([74]) Ustanovení čl. 23 odst. 1 zákona o ochraně osobních údajů.
([75]) Viz také příručka k zákonu o ochraně osobních údajů, kapitola III oddíl 2 k článku 23 (s. 157–164).
([76]) Tedy osobní údaje vyplývající z konkrétního technického zpracování údajů týkajících se fyzických či fyziologických znaků nebo znaků chování fyzické osoby za účelem jedinečné identifikace této osoby.
([77]) Nedodržení těchto požadavků může vést k sankcím podle čl. 71 bodu 3 zákona o ochraně osobních údajů.

15 a 17 zákona o ochraně osobních údajů a získá samostatný souhlas (tj. oddělený od souhlasu se zpracováním jiných osobních údajů), nebo kdy zpracování vyžaduje nebo povoluje zákon. Orgány veřejné správy mohou rovněž zpracovávat biometrické údaje, údaje o DNA získané genetickým testováním, osobní údaje odhalující rasový nebo etnický původ a údaje, které představují záznam v trestním rejstříku, z důvodů, které jsou k dispozici výlučně těmto orgánům (například je-li to nezbytné pro vyšetřování trestné činnosti nebo k tomu, aby soud projednal určitou věc) ([78]). Jako takové jsou právní základy pro zpracování citlivých údajů omezenější než u jiných druhů osobních údajů a jsou v korejském právu ještě přísnější než ty, které uvádí čl. 9 odst. 2 nařízení (EU) 2016/679.

(52) Kromě toho čl. 23 odst. 2 zákona o ochraně osobních údajů (jehož nedodržení může vést k sankcím ([79])) zdůrazňuje zvláštní význam zajištění náležitého zabezpečení při nakládání s citlivými údaji, aby u nich „nemohlo dojít ke ztrátě, odcizení, vyzrazení, padělání, pozměnění nebo poškození“. Jakkoli se jedná o obecný požadavek podle článku 29 zákona o ochraně osobních údajů, čl. 3 odst. 4 objasňuje, že úroveň zabezpečení musí být přizpůsobena druhu zpracovávaných osobních údajů, což znamená, že musí být vzata v úvahu konkrétní rizika spojená se zpracováním citlivých údajů. Zpracování údajů se navíc vždy provádí „způsobem, který minimalizuje možnost narušení“ soukromí subjektu údajů, a pokud možno „v anonymitě“ (čl. 3 odst. 6 a 7 zákona o ochraně osobních údajů). Tyto požadavky jsou zvláště důležité, pokud se zpracování týká citlivých údajů.

2.3.3 *Účelové omezení*

(53) Osobní údaje by měly být shromažďovány za konkrétním účelem, a to způsobem, který není neslučitelný s účelem zpracování.

(54) Tuto zásadu zajišťují ustanovení čl. 3 odst. 1 a 2 zákona o ochraně osobních údajů, podle nichž správce „upřesní a výslovně specifikuje“ účel zpracování, osobní údaje zpracovává vhodným způsobem nezbytným pro tento účel a nepoužije je nad rámec tohoto účelu. Obecná zásada účelového omezení je rovněž potvrzena v čl. 15 odst. 1, čl. 18 odst. 1, v článku 19 a v případě zpracovatelů (tzv. „externích subjektů zajišťujících zpracování“) v čl. 26 odst. 1 bodě 1 a odst. 5 a 7 zákona o ochraně osobních údajů. Zejména lze osobní údaje zpravidla používat a poskytovat třetím stranám pouze v rámci účelu, pro který byly shromážděny (čl. 15 odst. 1 a čl. 17 odst. 1 bod 2). Zpracování za slučitelným účelem, tj. „v rozsahu přiměřeně souvisejícím s původním účelem shromažďování“, může probíhat pouze tehdy, pokud negativně neovlivní dotčené subjekty údajů a pokud jsou přijata nezbytná bezpečnostní opatření (např. šifrování) (čl. 15 odst. 3 a čl. 17 odst. 4 zákona o ochraně osobních údajů). Aby bylo možné určit, zda je další zpracování prováděno za slučitelným účelem, uvádí prováděcí vyhláška k zákonu o ochraně osobních údajů konkrétní kritéria, která jsou obdobná těm, jež jsou uvedena v čl. 6 odst. 4 nařízení (EU) 2016/679, viz 36. bod odůvodnění.

(55) Jak je vysvětleno v 38. bodě odůvodnění, účelem shromažďování v případě korejských správců, kteří přijímají osobní údaje z Unie, je účel, za nímž jsou údaje předávány. Změna účelu správcem je povolena pouze výjimečně, ve zvláštních (vyjmenovaných) případech (čl. 18 odst. 2 body 1 až 3 zákona o ochraně osobních údajů, viz také 39. bod odůvodnění). Je-li změna účelu povolena zákonem, musí takové právní předpisy naopak respektovat základní právo na soukromí a ochranu údajů, jakož i zásady nezbytnosti a proporcionality stanovené v korejské ústavě. Kromě toho čl. 18 odst. 2 a 5 zákona o ochraně osobních údajů stanoví další záruky, zejména požadavek, podle něhož nesmí být takovou změnou účelu „nekorektním způsobem narušen zájem subjektu“, a je tudíž vždy zapotřebí vyvážení zájmů. To zajišťuje úroveň ochrany v zásadě rovnocennou úrovni ochrany podle čl. 5 odst. 1 písm. b) a článku 6 ve spojení s 50. bodem odůvodnění nařízení (EU) 2016/679.

2.3.4 *Přesnost a minimalizace údajů*

(56) Osobní údaje by měly být přesné a v případě potřeby aktualizované. Měly by rovněž být přiměřené, relevantní a omezené na to, co je nezbytné ve vztahu k účelům, pro které jsou zpracovávány.

([78]) Článek 18 prováděcí vyhlášky k zákonu o ochraně osobních údajů stanoví, že zde uvedené kategorie údajů jsou vyloučeny z ustanovení čl. 23 odst. 1 zákona, pokud je zpracovává veřejná instituce podle čl. 18 odst. 2 bodů 5 až 9 zákona o ochraně osobních údajů.

([79]) Viz čl. 73 bod 1 a čl. 75 odst. 2 bod 6 zákona o ochraně osobních údajů.

(57) Zásada přesnosti je obdobně uznána v čl. 3 odst. 3 zákona o ochraně osobních údajů, který vyžaduje, aby osobní údaje byly „přesné, úplné a aktuální v míře nezbytné ve vztahu k účelům“, pro které jsou zpracovávány. Minimalizace údajů je vyžadována podle čl. 3 odst. 1 a 6 a čl. 16 odst. 1 zákona o ochraně osobních údajů, které stanoví, že správce shromažďuje osobní údaje (pouze) „v minimálním rozsahu nezbytném“ pro dosažení zamýšleného účelu a v tomto ohledu nese důkazní břemeno. Je-li možné naplnit účel shromažďování zpracováním údajů v anonymizované podobě, měli by o ně správci usilovat (čl. 3 odst. 7 zákona o ochraně osobních údajů).

2.3.5 *Omezení uložení*

(58) Osobní údaje by měly být zpravidla uchovávány po dobu ne delší, než je nezbytné pro účely, pro které jsou osobní údaje zpracovávány.

(59) Zásada omezení uložení je obdobně stanovena v čl. 21 odst. 1 zákona o ochraně osobních údajů ([80]), který požaduje, aby správce neprodleně „zničil“ ([81]) osobní údaje po dosažení účelu zpracování, nebo po uplynutí doby uchovávání (podle toho, co nastane dříve), není-li další uchovávání vyžadováno zákonem ([82]). V takovém případě se příslušné osobní údaje „uchovávají a spravují odděleně od ostatních osobních údajů“ (čl. 21 odst. 3 zákona o ochraně osobních údajů).

(60) Ustanovení čl. 21 odst. 1 zákona o ochraně osobních údajů se nepoužije, pokud jsou pseudonymizované údaje zpracovávány pro účely statistiky, vědeckého výzkumu a archivace ve veřejném zájmu ([83]). Aby byla zajištěna zásada omezeného uchovávání údajů i v tomto případě, oznámení č. 2021-5 vyžaduje, aby správci anonymizovali údaje v souladu s článkem 58-2 zákona o ochraně osobních údajů, pokud tyto údaje nebyly po naplnění konkrétního účelu zpracování zničeny ([84]).

2.3.6 *Zabezpečení údajů*

(61) Osobní údaje by měly být zpracovávány způsobem, který zajišťuje jejich zabezpečení, včetně ochrany před neoprávněným nebo protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Za tímto účelem by podnikatelské subjekty měly přijmout vhodná technická nebo organizační opatření na ochranu osobních údajů před možnými hrozbami. Tato opatření by měla být posuzována s přihlédnutím ke stavu techniky, souvisejícím nákladům a k povaze, rozsahu, kontextu a účelům zpracování i k rizikům pro práva fyzických osob.

(62) Obdobnou zásadu zabezpečení stanoví čl. 3 odst. 4 zákona o ochraně osobních údajů, který uvádí, že správce osobních údajů „zajišťuje bezpečnou správu osobních údajů podle metod zpracování, druhů osobních údajů atd. s přihlédnutím k možnosti porušení práv subjektu údajů a k závažnosti příslušných rizik“. Kromě toho správce „zpracovává osobní údaje způsobem, který minimalizuje možnost narušení soukromí subjektu údajů“, a v této souvislosti se snaží zpracovávat osobní údaje pokud možno anonymně nebo v pseudonymizované podobě (čl. 3 odst. 6 a 7 zákona o ochraně osobních údajů).

(63) Tyto obecné požadavky jsou dále rozvedeny v článku 29 zákona o ochraně osobních údajů, podle kterého každý správce „přijme taková technická, řídicí a fyzická opatření, například vytvoření vnitřního plánu řízení a uchovávání záznamů o přihlášení atd., která jsou nezbytná k zajištění bezpečnosti a jsou předepsána

([80]) Článek 8 (ve spojení s článkem 8-2 prováděcí vyhlášky), článek 11 (ve spojení s čl. 12 odst. 2 prováděcí vyhlášky).
([81]) Metody ničení osobních údajů viz článek 16 prováděcí vyhlášky k zákonu o ochraně osobních údajů. Ustanovení čl. 21 odst. 2 zákona o ochraně osobních údajů objasňuje, že to zahrnuje „opatření nezbytná k zablokování obnovy“.
([82]) Nedodržení těchto požadavků může vést k trestním sankcím (čl. 73 odst. 1 a 2 zákona o ochraně osobních údajů). Článek 39-6 zákona o ochraně osobních údajů ukládá poskytovatelům informačních a komunikačních služeb další požadavek na výmaz osobních údajů uživatelů, kteří nevyužili nabízené informační a komunikační služby po dobu alespoň jednoho roku (pokud další uchovávání nevyžaduje zákon nebo o ně nepožádá daná fyzická osoba). Fyzické osoby musí být informovány o zamýšleném výmazu jejich údajů 30 dní před uplynutím jednoleté lhůty (článek 39-6 odst. 2 zákona o ochraně osobních údajů a čl. 48-5 odst. 3 prováděcí vyhlášky k zákonu o ochraně osobních údajů). Vyžaduje-li další uchovávání zákon, musí být uchovávané údaje uloženy odděleně od ostatních údajů uživatelů a mohou být použity nebo zpřístupněny pouze v souladu s tímto zákonem (čl. 48-5 odst. 1 a 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů).
([83]) Článek 28-7 zákona o ochraně osobních údajů.
([84]) Oznámení č. 2021-5 (příloha I), oddíl 4.

prezidentskou vyhláškou, aby nemohlo dojít ke ztrátě, odcizení, vyzrazení, padělání, pozměnění nebo poškození osobních údajů“. Ustanovení čl. 30 odst. 1 prováděcí vyhlášky k zákonu o ochraně osobních údajů specifikuje tato opatření odkazem na 1) vypracování a provedení vnitřního plánu řízení pro bezpečné zpracování osobních údajů; 2) kontroly a omezení přístupu; 3) přijetí šifrovací technologie pro bezpečné ukládání a předávání osobních údajů; 4) záznamy o přihlášení; 5) bezpečnostní programy a 6) fyzická opatření, jako je bezpečné úložiště nebo systém zámku ([85]).

(64) Kromě toho platí zvláštní povinnosti v případě, že dojde k porušení zabezpečení údajů (článek 34 zákona o ochraně osobních údajů ve spojení s články 39 a 40 prováděcí vyhlášky k zákonu o ochraně osobních údajů) ([86]). Správce je zejména povinen neprodleně oznámit dotčeným subjektům údajů podrobnosti o porušení zabezpečení ([87]), včetně informací o (povinných) protiopatřeních přijatých správcem a o tom, co mohou subjekty údajů učinit, aby minimalizovaly riziko škody (čl. 34 odst. 1 a 2 zákona o ochraně osobních údajů) ([88]). Pokud se porušení zabezpečení údajů týká alespoň 1 000 subjektů údajů, správce neprodleně oznámí porušení zabezpečení údajů a přijatá protiopatření rovněž Komisi pro ochranu osobních údajů a Korejské agentuře pro internet a zabezpečení, která může poskytnout technickou pomoc (čl. 34 odst. 3 zákona o ochraně osobních údajů ve spojení s článkem 39 prováděcí vyhlášky k zákonu o ochraně osobních údajů). Správci odpovídají za škodu způsobenou porušením zabezpečení údajů v souladu s ustanoveními občanského zákoníku o odpovědnosti za delikty (viz také oddíl 2.5, opravné prostředky) ([89]).

(65) Při plnění jeho povinností v oblasti zabezpečení musí být správci nápomocen pověřenec pro ochranu soukromí, mezi jehož úkoly patří mimo jiné budování vnitřního kontrolního systému, „který má zabránit vyzrazení, zneužití a neoprávněnému použití osobních údajů“ (čl. 31 odst. 2 bod 4 zákona o ochraně osobních údajů). Správce má navíc povinnost provádět „náležitou kontrolu a dohled“ nad svými zaměstnanci, kteří zpracovávají osobní údaje, a to i pokud jde o bezpečné nakládání s těmito údaji; to zahrnuje nezbytnou odbornou přípravu („vzdělávání“) zaměstnanců (článek 28 odst. 1 a 2 zákona o ochraně osobních údajů). A konečně v případě dílčího zpracování musí správce stanovit vůči „externímu subjektu zajišťujícímu zpracování“ požadavky týkající se mimo jiné bezpečného nakládání s osobními údaji („technické a řídicí záruky“) a prostřednictvím inspekcí musí dohlížet na to, jak jsou tyto záruky prováděny (čl. 26 odst. 1 a 4 zákona o ochraně osobních údajů ve spojení s čl. 28 odst. 1 body 3, 4 a 6 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

2.3.7 *Transparentnost*

(66) Subjekty údajů by měly být informovány o hlavních znacích zpracování jejich osobních údajů.

([85]) Pokud jde o zpracování osobních údajů poskytovateli informačních a komunikačních služeb, článek 39-5 zákona o ochraně osobních údajů výslovně stanoví, že počet osob, které nakládají s osobními informacemi uživatelů, je omezen na minimum. Poskytovatelé informačních a komunikačních služeb navíc zajistí, aby osobní údaje uživatelů nebyly prostřednictvím informační a komunikační sítě přístupné veřejnosti (čl. 39-10 odst. 1 zákona o ochraně osobních údajů). Zpřístupněné informace musí být na žádost Komise pro ochranu osobních údajů vymazány nebo zablokovány (čl. 39-10 odst. 2 zákona o ochraně osobních údajů). Obecněji lze říci, že poskytovatelé informačních a komunikačních služeb (a třetí strany, které přijímají osobní údaje uživatelů) podléhají dalším bezpečnostním povinnostem, které upřesňuje článek 48-2 prováděcí vyhlášky k zákonu o ochraně osobních údajů, např. vypracování a zavedení vnitřního plánu řízení týkajícího se bezpečnostních opatření, opatření k zajištění kontroly přístupu, šifrování, použití softwaru k detekci škodlivých programů atd.

([86]) Kromě toho existuje obecný zákaz poškozování, ničení, pozměňování, padělání nebo úniku osobních údajů bez zákonného oprávnění, viz čl. 59 bod 3 zákona o ochraně osobních údajů.

([87]) Požadavek na informování fyzické osoby se nepoužije v případech, kdy dojde k porušení zabezpečení údajů týkajícímu se pseudonymizovaných údajů zpracovávaných pro účely statistiky, vědeckého výzkumu nebo archivace ve veřejném zájmu (článek 28-7 zákona o ochraně osobních údajů, který stanoví výjimku z čl. 34 odst. 1 a článku 39-4 zákona o ochraně osobních údajů). Zajištění individuálního oznámení by vyžadovalo, aby dotčený správce identifikoval fyzickou osobu v rámci pseudonymizovaného datového souboru, což je podle článku 28-5 zákona o ochraně osobních údajů výslovně zakázáno. Obecná povinnost oznamovat porušení zabezpečení údajů (Komisi pro ochranu osobních údajů) však nadále platí.

([88]) Oznamovací povinnosti včetně načasování a možnosti oznámení „po etapách“ dále specifikuje článek 40 prováděcí vyhlášky k zákonu o ochraně osobních údajů. Přísnější pravidla se použijí na poskytovatele informačních a komunikačních služeb, kteří jsou povinni informovat subjekt údajů a Komisi pro ochranu osobních údajů do 24 hodin poté, co zjistí, že došlo ke ztrátě, odcizení nebo úniku osobních údajů (článek 39-4 odst. 1 zákona o ochraně osobních údajů). Toto oznámení musí uvádět podrobnosti o osobních údajích, které unikly, okamžik, kdy k úniku došlo, opatření, která může uživatel přijmout, opatření přijatá poskytovatelem v reakci na únik a kontaktní údaje oddělení, na které se uživatel může obrátit s dotazy (čl. 39-4 odst. 1 body 1 až 5 zákona o ochraně osobních údajů). Pokud existuje ospravedlnitelný důvod, např. nejsou k dispozici kontaktní údaje uživatele, lze použít jiné způsoby oznámení, např. zveřejněním informací na internetových stránkách (čl. 39-4 odst. 1 zákona o ochraně osobních údajů ve spojení s čl. 48-4 odst. 4 a násl. prováděcí vyhlášky k zákonu o ochraně osobních údajů). V takovém případě musí být o důvodech informována Komise pro ochranu osobních údajů (čl. 34-4 odst. 3 zákona o ochraně osobních údajů).

([89]) Viz např. rozhodnutí Nejvyššího soudu 2011Da59834, 2011Da59858 a 2011Da59841, 26. prosince 2012. Shrnutí v anglickém jazyce je k dispozici na adrese: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) To je v korejském systému zajištěno různými způsoby. Vedle práva na informace podle čl. 4 bodu 1 (obecně) a čl. 20 odst. 1 zákona o ochraně osobních údajů (pokud jde o osobní údaje shromážděné od třetích stran), jakož i práva na přístup podle článku 35 zákona o ochraně osobních údajů zahrnuje zákon o ochraně osobních údajů i obecný požadavek na transparentnost, pokud jde o účel zpracování (čl. 3 odst. 1 zákona o ochraně osobních údajů) a specifické požadavky na transparentnost v případě, kdy je zpracování založeno na souhlasu (čl. 15 odst. 2, čl. 17 odst. 2 a čl. 18 odst. 3 zákona o ochraně osobních údajů) ([90]). Kromě toho čl. 20 odst. 2 zákona o ochraně osobních údajů vyžaduje, aby někteří správci (ti, u nichž zpracování překračuje určité prahové hodnoty ([91])) oznámili subjektu údajů, jehož osobní údaje obdrželi od třetí strany, zdroj informací, účel zpracování a právo subjektu údajů požadovat pozastavení zpracování, ledaže se takové oznámení ukáže jako nemožné z důvodu nedostatku jakýchkoli kontaktních údajů. Výjimky se vztahují na určité soubory osobních údajů uchovávané orgány veřejné správy, zejména na soubory, které obsahují údaje zpracovávané pro účely národní bezpečnosti, pro účely jiných zvláště důležitých („závažných“) národních zájmů nebo pro účely vymáhání trestního práva, nebo pokud by oznámení mohlo způsobit újmu na životě či zdraví jiné osoby nebo nekorektním způsobem působilo škodu na majetku a jiných zájmech jiné osoby, pouze však v případě, kdy jsou dotčené veřejné nebo soukromé zájmy „zjevně nadřazeny“ právům dotčených subjektů údajů (čl. 20 odst. 4 zákona o ochraně osobních údajů). Tento postup vyžaduje vyvažování zájmů.

(68) Kromě toho čl. 3 odst. 5 zákona o ochraně osobních údajů předepisuje, že správci zveřejní své zásady ochrany soukromí (a další záležitosti související se zpracováním osobních údajů). Tento požadavek je dále upřesněn v článku 30 zákona o ochraně osobních údajů ve spojení s článkem 31 prováděcí vyhlášky k zákonu o ochraně osobních údajů. Podle těchto ustanovení musí zásady ochrany soukromí mimo jiné zahrnovat 1) druhy zpracovávaných osobních údajů; 2) účel zpracování; 3) dobu uchovávání; 4) zda jsou osobní údaje poskytovány třetí straně ([92]); 5) případné dílčí zpracování; 6) informace o právech subjektu údajů a způsobu jejich uplatnění a 7) kontaktní údaje (včetně jména pověřence pro ochranu soukromí nebo interního oddělení odpovědného za zajištění souladu s údaji pravidla ochrany údajů a vyřizování stížností). Zásady ochrany osobních údajů musí být veřejně dostupné takovým způsobem, aby je subjekty údajů „mohly snadno rozpoznat“ (čl. 30 odst. 2 zákona o ochraně osobních údajů) ([93]), a musí být průběžně aktualizovány (čl. 31 odst. 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

(69) Veřejné instituce podléhají další povinnosti registrovat u Komise pro ochranu osobních údajů zejména následující informace: 1) název veřejné instituce; 2) důvody a účely zpracování souborů osobních údajů; 3) podrobnosti o osobních údajích, které jsou zaznamenány; 4) způsob zpracování; 5) dobu uchovávání; 6) počet subjektů údajů, jejichž osobní údaje jsou uchovávány; 7) oddělení, které vyřizuje žádosti subjektů údajů, a 8) příjemce osobních údajů, pokud jsou údaje poskytovány běžně nebo opakovaně (čl. 32 odst. 1 zákona o ochraně osobních údajů) ([94]). Registrované soubory osobních údajů zveřejňuje Komise pro ochranu osobních údajů a musí na ně odkazovat i veřejné instituce ve svých zásadách ochrany soukromí (čl. 30 odst. 1 a čl. 32 odst. 4 zákona o ochraně osobních údajů).

(70) V zájmu zvýšení transparentnosti pro subjekty údajů v Unii, jejichž osobní údaje jsou předávány do Koreje na základě tohoto rozhodnutí, ukládají body i) a ii) oddílu 3 oznámení č. 2021-5 (příloha I) další požadavky na transparentnost. Zaprvé musí při přijímání osobních údajů z Unie na základě tohoto rozhodnutí korejští správci bez zbytečného odkladu (a v každém případě nejpozději do jednoho měsíce od předání) oznámit dotčeným subjektům údajů jména a kontaktní údaje subjektů, které údaje předávají a přijímají, předávané osobní

([90]) Zejména pokud jsou osobní údaje zpracovávány se souhlasem fyzické osoby, musí správce této fyzické osobě sdělit účel zpracování, podrobnosti o údajích, které mají být zpracovány, příjemce údajů, dobu, po kterou jsou osobní údaje uchovávány a používány, stejně jako skutečnost, že fyzická osoba je oprávněna souhlas odepřít (a případná znevýhodnění, která z toho mohou vyplývat).

([91]) Podle čl. 15-2 odst. 1 prováděcí vyhlášky k zákonu o ochraně osobních údajů se to týká správců zpracovávajících citlivé informace nejméně 50 000 subjektů údajů nebo „běžné“ osobní údaje nejméně jednoho milionu subjektů údajů. Ustanovení čl. 15-2 odst. 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů uvádí metody a načasování oznámení, čl. 15-2 odst. 3 stanoví požadavek na vedení určitých záznamů o oznámení. Kromě toho platí zvláštní pravidla pro určité kategorie poskytovatelů informačních a komunikačních služeb (těch, kteří v předchozím roce vygenerovali tržby z prodeje ve výši nejméně 10 miliard wonů, nebo těch, kteří uchovávají/spravují osobní údaje v průměru alespoň jednoho milionu uživatelů denně během tři měsíců před koncem předchozího roku), kteří jsou povinni pravidelně informovat uživatele o historii používání jejich osobních údajů, ledaže se takové informování ukáže jako nemožné z důvodu nedostatku jakýchkoli kontaktních informací (článek 39-8 zákona o ochraně osobních údajů a článek 48-6 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

([92]) Podle informací obdržených od korejské vlády to znamená povinnost jednotlivě uvést příjemce v zásadách ochrany soukromí.

([93]) Další možnosti jsou uvedeny v čl. 31 odst. 3 prováděcí vyhlášky k zákonu o ochraně osobních údajů.

([94]) Požadavek registrace se nevztahuje na určité druhy souborů osobních údajů, například soubory, které zaznamenávají záležitosti související s národní bezpečností, diplomatickým tajemstvím, vyšetřováním trestných činů, trestním stíháním, tresty, vyšetřováním trestných činů souvisejících s daněmi, nebo soubory, které se týkají výhradně interního plnění pracovních úkolů (čl. 32 odst. 2 zákona o ochraně osobních údajů).

údaje (nebo kategorie osobních údajů), účel shromažďování korejským správcem, dobu uchovávání a práva, která jsou dostupná podle zákona o ochraně osobních údajů. Zadruhé, při poskytování osobních údajů přijatých z Unie na základě tohoto rozhodnutí třetím stranám musí být subjekty údajů informovány mimo jiné o příjemci, osobních údajích nebo kategoriích osobních údajů, které mají být poskytnuty, o zemi, do které jsou údaje poskytovány (je-li to relevantní), stejně jako o právech, která jsou dostupná podle zákona o ochraně osobních údajů ([95]). Oznámení tak zajišťuje, že fyzické osoby z EU budou i nadále informovány o konkrétních správcích zpracovávajících jejich údaje a budou moci uplatňovat svá práva vůči příslušným subjektům.

(71) Oddíl 3 bod iii) oznámení (příloha I) umožňuje určité omezené a kvalifikované výjimky z těchto dodatečných povinností týkajících se transparentnosti, které jsou v zásadě rovnocenné těm, které stanoví nařízení (EU) 2016/679. Informování subjektů údajů v Unii není vyžadováno, 1) pokud a dokud je nezbytné omezit oznamování z určitých důvodů veřejného zájmu (například pokud jsou informace zpracovávány pro účely národní bezpečnosti nebo probíhajícího vyšetřování trestné činnosti), jsou-li tyto cíle veřejného zájmu zjevně nadřazeny právům subjektu údajů; 2) subjekt údajů již uvedené informace má; 3) pokud a dokud je pravděpodobné, že oznámení způsobí újmu na životě nebo zdraví daného jednotlivce nebo jakékoli jiné osoby nebo nekorektním způsobem poškodí majetkové zájmy jiné osoby, pokud jsou tato práva nebo zájmy zjevně nadřazeny právům subjektu údajů; nebo 4) pokud nejsou k dispozici kontaktní údaje dotčených fyzických osob nebo by informování těchto osob vyžadovalo nepřiměřené úsilí. Při určování toho, zda je možné kontaktovat subjekt údajů nebo zda to vyžaduje nadměrné úsilí, by měla být vzata v úvahu možnost spolupracovat s vývozcem údajů v Unii.

(72) Pravidla v 67. až 71. bodě odůvodnění tudíž zajišťují v zásadě rovnocennou úroveň ochrany s ohledem na transparentnost, jakou stanoví nařízení (EU) 2016/679.

2.3.8 *Individuální práva*

(73) Subjekty údajů by měly mít určitá práva, která lze vůči správci nebo zpracovateli vymáhat, zejména právo na přístup k údajům, právo na opravu, právo podat námitku proti zpracování a právo na výmaz údajů. Tato práva mohou zároveň podléhat omezením, pokud jsou tato omezení nezbytná a přiměřená k zajištění důležitých cílů obecného veřejného zájmu.

(74) Podle čl. 3 odst. 5 zákona o ochraně osobních údajů správce zaručí práva subjektu údajů vyjmenovaná v článku 4 zákona o ochraně osobních údajů a dále upřesněná v článcích 35 až 37, 39 a 39-2 zákona o ochraně osobních údajů.

(75) Zaprvé mají fyzické osoby právo na informace a přístup. Pokud správce shromáždil osobní údaje od třetí strany (jak tomu bude vždy v případě předání údajů z Unie), mají subjekty údajů obecně právo získat informace o 1) „zdroji“ shromážděných osobních údajů (tj. převodci); 2) účelu zpracování a 3) právu subjektu údajů požadovat pozastavení zpracování (čl. 20 odst. 1 zákona o ochraně osobních údajů). Platí omezené výjimky, a to v případech, kdy by oznámení mohlo způsobit újmu na životě či zdraví jiné osoby nebo „nekorektním způsobem poškodit majetek a jiné zájmy“ jiné osoby, pouze však v případě, kdy tyto zájmy třetí strany „výslovně nadřazeny“ právům dotčeného subjektu údajů (čl. 20 odst. 4 bod 2 zákona o ochraně osobních údajů).

(76) Kromě toho čl. 35 odst. 1 a 3 zákona o ochraně osobních údajů ve spojení s čl. 41 odst. 4 prováděcí vyhlášky k zákonu o ochraně osobních údajů poskytuje subjektům údajů právo na přístup k jejich osobním údajům ([96]). Právo na přístup zahrnuje potvrzení o zpracování, informace o druhu zpracovávaných údajů, účelu zpracování, době uchovávání, jakož i případném zpřístupnění třetí straně a poskytnutí kopie zpracovávaných osobních údajů

([95]) Oznámení č. 2021-5, oddíl 3 bod ii) (příloha I).

([96]) Podle čl. 35 odst. 3 zákona o ochraně osobních údajů ve spojení s čl. 42 odst. 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů může správce odložit přístup z „řádného důvodu“ (tj. z oprávněných důvodů, např. pokud je zapotřebí více času na posouzení toho, zda lze přístup poskytnout), musí však do deseti dnů toto odůvodnění sdělit subjektu údajů a poskytnout mu informace, jak proti tomuto rozhodnutí podat opravný prostředek; jakmile důvod odkladu pomine, musí být přístup umožněn.

(čl. 4 bod 3 zákona o ochraně osobních údajů ve spojení s čl. 41 odst. 1 prováděcí vyhlášky k zákonu o ochraně osobních údajů) ([97]). Přístup může být omezen (částečný přístup) ([98]) nebo odepřen pouze tehdy, je-li to stanoveno zákonem ([99]), pokud by to pravděpodobně způsobilo újmu na životě nebo zdraví třetí strany nebo by to pravděpodobně vedlo k neoprávněnému narušení majetkových a jiných zájmů jiné osoby (čl. 35 odst. 4 zákona o ochraně osobních údajů) ([100]). Z posledně uvedeného vyplývá, že je třeba provádět vyvažování mezi ústavně chráněnými právy a svobodami jednotlivce na jedné straně a jiných osob na straně druhé. Je-li přístup omezen nebo odepřen, musí správce informovat subjekt údajů o příslušných důvodech a o způsobu podání opravného prostředku proti rozhodnutí (čl. 41 odst. 5 a čl. 42 odst. 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

(77) Zadruhé mají subjekty údajů právo na opravu nebo výmaz ([101]) svých osobních údajů, „pokud jiné právní předpisy výslovně nestanoví jinak“ (čl. 36 odst. 1 a 2 zákona o ochraně osobních údajů) ([102]). Po obdržení žádosti musí správce věc neprodleně prošetřit, přijmout nezbytná opatření ([103]) a do deseti dnů o nich vyrozumět subjekt údajů; nelze-li žádosti vyhovět, zahrnuje tato oznamovací povinnost důvody zamítnutí a způsob podání opravného prostředku (viz čl. 36 odst. 4 zákona o ochraně osobních údajů ve spojení s čl. 43 odst. 3 prováděcí vyhlášky k zákonu o ochraně osobních údajů) ([104]).

(78) A konečně mají také subjekty údajů právo na okamžité pozastavení zpracování jejich osobních údajů ([105]), pokud se nepoužije jedna z vyjmenovaných výjimek (čl. 37 odst. 1 a 2 zákona o ochraně osobních údajů) ([106]). Správce může žádost zamítnout, 1) pokud je to výslovně povoleno zákonem nebo je to nezbytné („nevyhnutelné“) ke splnění zákonných povinností; 2) pokud by pozastavení zpracování pravděpodobně způsobilo újmu na životě nebo zdraví třetí strany nebo neoprávněné narušení majetkových a jiných zájmů jiné osoby; 3) pokud by veřejná instituce bez zpracování údajů nemohla plnit svou zákonem stanovenou funkci nebo 4) pokud subjekt údajů výslovně neukončí příslušnou základní smlouvu se správcem, přestože by bez takového zpracování údajů nebylo možné smlouvu plnit. V takovém případě musí správce neprodleně oznámit subjektu údajů důvody zamítnutí a způsob podání opravného prostředku (čl. 37 odst. 2 zákona o ochraně osobních údajů ve spojení s čl. 44 odst. 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů). Podle čl. 37 odst. 4 zákona o ochraně osobních údajů musí správce při vyhovění žádosti o pozastavení zpracování neprodleně „přijmout nezbytná opatření včetně zničení příslušných osobních údajů“ ([107]).

(79) Právo na pozastavení zpracování existuje i v případech, kdy jsou osobní údaje používány pro účely přímého marketingu, tedy za účelem propagace zboží nebo služeb nebo žádostí o jejich koupi. Navíc takové další zpracování obecně vyžaduje zvláštní (dodatečný) souhlas subjektu údajů (viz čl. 15 odst. 1 bod 1, čl. 17 odst. 2 bod 1 zákona o ochraně osobních údajů) ([108]). Při žádosti o tento souhlas musí správce informovat subjekt údajů zejména o zamýšleném použití údajů pro účely přímého marketingu (tj. o tom, že jej lze kontaktovat za účelem

([97]) Přístup k osobním údajům zpracovávaným veřejnou institucí lze získat přímo od instituce nebo nepřímo podáním žádosti ke Komisi pro ochranu osobních údajů, která žádost neprodleně předá (čl. 35 odst. 2 zákona o ochraně osobních údajů a čl. 41 odst. 3 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

([98]) Podle čl. 42 odst. 1 prováděcí vyhlášky k zákonu o ochraně osobních údajů je správce povinen poskytnout částečný přístup, pokud se alespoň části údajů netýkají důvody pro odmítnutí.

([99]) Takový právní předpis musí naopak respektovat základní právo na soukromí a ochranu údajů, jakož i zásady nezbytnosti a proporcionality stanovené v korejské ústavě.

([100]) Kromě toho mohou veřejné instituce odmítnout poskytnutí přístupu, pokud by to způsobilo závažné potíže při provádění určitých funkcí, včetně probíhajících auditů nebo vyměřování, výběru nebo vracení daní (čl. 35 odst. 4 zákona o ochraně osobních údajů).

([101]) V tomto případě musí správce přijmout opatření, která zabrání obnovení osobních údajů, viz čl. 36 odst. 3 zákona o ochraně osobních údajů.

([102]) Takové právní předpisy musí splňovat požadavky ústavy, podle nichž lze základní právo omezit pouze tehdy, je-li to nezbytné pro národní bezpečnost nebo pro zachování práva a pořádku v zájmu veřejného blaha, a toto omezení se nesmí dotýkat podstaty svobody nebo práva (čl. 37 odst. 2 ústavy).

([103]) Ustanovení čl. 43 odst. 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů stanoví zvláštní postup v případě, že správce zpracovává soubory osobních informací poskytnuté jiným správcem.

([104]) Nepřijetí nezbytných opatření k opravě nebo vymazání osobních údajů a další používání nebo poskytnutí těchto údajů třetí straně může vést k trestním sankcím (čl. 73 odst. 2 zákona o ochraně osobních údajů).

([105]) Podle čl. 44 odst. 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů správce do deseti dnů od obdržení žádosti informuje subjekt údajů o tom, že řádně pozastavil zpracování.

([106]) Pokud jde o veřejné instituce, lze právo na pozastavení zpracování uplatnit u údajů obsažených v registrovaných souborech osobních údajů (článek 37 ve spojení s článkem 32 zákona o ochraně osobních údajů). Tato registrace není vyžadována v omezeném počtu situací, např. pokud se soubory osobních údajů týkají národní bezpečnosti, vyšetřování trestné činnosti, diplomatických vztahů atd. (čl. 32 odst. 2 zákona o ochraně osobních údajů).

([107]) Nepozastavení zpracování může vést k trestním sankcím (čl. 73 odst. 3 zákona o ochraně osobních údajů).

([108]) Mediační výbor (viz 133. bod odůvodnění) se zabýval několika případy, kdy si fyzické osoby stěžovaly na použití svých údajů pro účely přímého marketingu bez jejich souhlasu, a výsledkem bylo například vyplacení náhrady škody a výmaz osobních údajů příslušným správcem (viz např. mediační výbor 20R10-024(2020.11.18), 20R08-015(2020.8.28), 20R07-031(2020.9.1)).

propagace zboží nebo služeb nebo žádosti o jejich koupi) „výslovně rozpoznatelným způsobem“ (čl. 22 odst. 2 a 4 zákona o ochraně osobních údajů ve spojení s čl. 17 odst. 2 bodem 1 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

(80) Aby usnadnil výkon individuálních práv, musí správce zavést vyhrazené postupy a veřejně je oznámit (čl. 38 odst. 4 zákona o ochraně osobních údajů) ([109]). To zahrnuje postupy pro vznesení námitek proti zamítnutí žádosti (čl. 38 odst. 5 zákona o ochraně osobních údajů). Správce musí zajistit, aby postup pro výkon práv byl „k subjektu údajů vstřícný“ a nebyl obtížnější než postup při shromažďování osobních údajů; to zahrnuje i povinnost poskytovat informace o tomto postupu na internetových stránkách správce (čl. 41 odst. 2, čl. 43 odst. 1 a čl. 44 odst. 1 prováděcí vyhlášky k zákonu o ochraně osobních údajů) ([110]). Fyzické osoby mohou k podání takové žádosti zmocnit zástupce (čl. 38 odst. 1 zákona o ochraně osobních údajů ve spojení s článkem 45 prováděcí vyhlášky k zákonu o ochraně osobních údajů). Ačkoli je správce oprávněn účtovat poplatek (a v případě žádosti o zaslání kopií osobních údajů poštou i poštovné), částka musí být stanovena „v mezích skutečných nákladů nezbytných pro zpracování [žádosti]“; nelze účtovat žádný poplatek (ani poštovné), pokud podnět k žádosti dal správce (článek 38 odst. 3 zákona o ochraně osobních údajů ve spojení s článkem 47 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

(81) Zákon o ochraně osobních informací a příslušná prováděcí vyhláška neobsahují obecná ustanovení řešící vydávání rozhodnutí, která se dotýkají subjektu údajů a jsou založena výhradně na automatizovaném zpracování osobních údajů. Pokud však jde o osobní údaje, které byly shromážděny v Unii, jakékoli rozhodnutí založené na automatizovaném zpracování bude obvykle činit správce v Unii (který má přímý vztah s dotyčným subjektem údajů), a vztahuje se tedy na něj nařízení (EU) 2016/679 ([111]). To zahrnuje situace předávání, kdy zpracování provádí zahraniční (např. korejský) podnikatelský subjekt jednající jako zprostředkovatel (zpracovatel) jménem správce v Unii (nebo jako externí zpracovatel jednající jménem zpracovatele z Unie, jenž získal údaje od správce v Unii, který je shromáždil), který na tomto základě činí rozhodnutí. Neexistence zvláštních pravidel pro automatizované rozhodování v zákoně o ochraně osobních údajů tedy pravděpodobně neovlivní úroveň ochrany osobních údajů předávaných podle tohoto rozhodnutí.

(82) Ustanovení týkající se transparentnosti v případě žádosti (článek 20) a individuálních práv (články 35 až 37), jakož i individuální oznamovací povinnost u poskytovatelů informačních a komunikačních služeb (článek 39-8 zákona o ochraně osobních údajů) se výjimečně nepoužijí u pseudonymizovaných údajů, pokud jsou zpracovávány pro účely statistiky, vědeckého výzkumu nebo archivace ve veřejném zájmu (článek 28-7 zákona o ochraně osobních údajů) ([112]). V souladu s přístupem podle čl. 11 odst. 2 (ve spojení s 57. bodem odůvodnění) nařízení (EU) 2016/679 je to odůvodněno tím, že v zájmu zajištění transparentnosti nebo udělení individuálních práv by správce musel zjistit, zda některé údaje (a pokud ano, které) souvisí s fyzickou osobou, která žádost podává, což je podle zákona o ochraně osobních údajů (čl. 28-5 odst. 1) výslovně zakázáno. Pokud navíc tato opětovná identifikace zahrnuje zrušení pseudonymizace celého (pseudonymizovaného) datového souboru, vystavila by osobní informace všech ostatních dotčených osob zvýšeným rizikům. Zatímco nařízení (EU) 2016/679 odkazuje na situace, kdy je opětovná identifikace prakticky nemožná, zákon o ochraně osobních údajů zaujímá přísnější přístup a výslovně zakazuje opětovnou identifikaci ve všech situacích, kdy jsou zpracovávány pseudonymizované údaje.

(83) Korejský systém popsaný v 74. až 82. bodě odůvodnění tudíž obsahuje pravidla o právech subjektů údajů, která poskytují úroveň ochrany v zásadě rovnocennou ochraně podle nařízení (EU) 2016/679.

([109]) Viz také čl. 30 odst. 1 bod 5 zákona o ochraně osobních údajů o zásadách ochrany osobních údajů, který mimo jiné uvádí informace o právech, která náleží fyzické osobě, a o způsobu jejich uplatnění.

([110]) Viz také čl. 39-7 odst. 2 zákona o ochraně osobních údajů, pokud jde o poskytovatele informačních a komunikačních služeb.

([111]) Naproti tomu ve výjimečném případě, kdy má korejský podnikatelský subjekt přímý vztah se subjektem údajů z EU, to obvykle bude důsledek jeho cíleného zaměření na fyzickou osobu v Evropské unii, které nabízí zboží nebo služby nebo monitoruje její chování. V tomto případě bude korejský podnikatelský subjekt sám spadat do oblasti působnosti nařízení (EU) 2016/679 (čl. 3 odst. 2), a musí tedy přímo dodržovat právní předpisy EU na ochranu údajů.

([112]) Viz také oznámení č. 2021-5, které potvrzuje, že oddíl III zákona o ochraně osobních údajů (včetně článku 28-7) se použije pouze v případě, že jsou pseudonymizované údaje zpracovávány pro vědecký výzkum, statistiky nebo archivaci ve veřejném zájmu, viz oddíl 4 přílohy I tohoto rozhodnutí.

2.3.9 *Další předávání*

(84) Úroveň ochrany osobních údajů předávaných z Unie správcům v Korejské republice nesmí být oslabena dalším předáváním těchto údajů příjemcům v třetí zemi.

(85) Taková „další předání" z pohledu korejského správce představují mezinárodní předání z Korejské republiky. V tomto ohledu zákon o ochraně osobních údajů rozlišuje mezi zadáním zpracování externímu subjektu zajišťujícímu zpracování (tj. zpracovateli) a poskytnutím osobních údajů třetím stranám ([113]).

(86) Zaprvé, pokud je zpracování osobních údajů zadáno externímu subjektu se sídlem v třetí zemi, musí korejský správce zajistit soulad s ustanoveními zákona o ochraně osobních údajů týkajícími se zadání činnosti externímu subjektu (článek 26 zákona o ochraně osobních údajů). To zahrnuje zavedení právně závazného nástroje, který mimo jiné omezuje zpracování zadané externímu subjektu na účel externě zajišťované činnosti, ukládá technické a řídicí záruky a omezuje dílčí zpracování (viz čl. 26 odst. 1 zákona o ochraně osobních údajů); a zveřejňování informací o práci zadané externímu subjektu. Dále je správce povinen „poučit" externí subjekt zajišťující zpracování o nezbytných bezpečnostních opatřeních a dohlížet, a to i prostřednictvím inspekcí, zda subjekt plní všechny povinnosti správce podle zákona o ochraně osobních údajů ([114]) i podle smlouvy o zajištění externího zpracování.

(87) Pokud externí subjekt zajišťující zpracování způsobí škodu zpracováním osobních údajů v rozporu se zákonem o ochraně osobních údajů, ponese odpovědnost správce, stejně jako by tomu bylo v případě zaměstnanců správce (čl. 26 odst. 6 zákona o ochraně osobních údajů). Korejský správce proto nadále nese odpovědnost za osobní údaje, jejichž zpracování je zadáno externímu subjektu, a musí zajistit, aby zahraniční zpracovatel zpracovával údaje v souladu se zákonem o ochraně osobních údajů. Pokud externí subjekt zajišťující zpracování zpracovává informace v rozporu se zákonem o ochraně osobních údajů, může korejský správce nést odpovědnost za nesplnění své povinnosti zajistit soulad se zákonem o ochraně osobních údajů, například prostřednictvím svého dohledu nad externím subjektem zajišťujícím zpracování. Záruky obsažené ve smlouvě o zajištění externího zpracování a odpovědnost korejského správce za kroky externího subjektu zajišťujícího zpracování zajišťují kontinuitu ochrany, pokud je zpracování osobních údajů zadáno externímu subjektu mimo Koreu.

(88) Zadruhé mohou korejští správci poskytnout osobní údaje třetí straně se sídlem mimo Koreu. Zákon o ochraně osobních údajů obsahuje řadu právních důvodů, které obecně umožňují poskytování údajů třetím stranám, pokud má třetí strana sídlo mimo Koreu, správce však v zásadě ([115]) musí získat souhlas subjektu údajů ([116]) poté, co subjektu údajů sdělí 1) druh osobních údajů; 2) příjemce osobních údajů; 3) účel předání ve smyslu účelu zpracování sledovaného příjemcem; 4) dobu uchovávání příjemcem pro účely zpracování a rovněž 5) skutečnost, že subjekt údajů může souhlas odepřít (čl. 17 odst. 2 a 3 zákona o ochraně osobních údajů). Oznámení č. 2021-5 ve svém oddílu věnovaném transparentnosti (viz 70. bod odůvodnění) vyžaduje, aby byly fyzické osoby informovány o třetí zemi, do níž budou jejich údaje poskytnuty. Tím je zajištěno, že subjekty údajů v Unii mohou učinit plně informované rozhodnutí, zda udělí nebo neudělí souhlas s poskytnutím do zahraničí. Správce navíc nesmí uzavřít smlouvu s příjemcem, který je třetí stranou, v rozporu se zákonem o ochraně osobních údajů, což znamená, že smlouva nesmí obsahovat povinnosti, které by byly v rozporu s povinnostmi, jež zákon o ochraně osobních údajů ukládá správci ([117]).

([113]) Na poskytovatele informačních a komunikačních služeb se vztahují zvláštní pravidla. V souladu s článkem 39-12 zákona o ochraně osobních údajů musí poskytovatelé informačních a komunikačních služeb zpravidla získat souhlas uživatele pro jakékoli předání osobních údajů do zahraničí. V případě, že jsou osobní údaje předávány v rámci zadání operací zpracování externímu subjektu, včetně uchovávání, není souhlas vyžadován, pokud byly dotčeným osobám přímo nebo prostřednictvím veřejného oznámení umožňujícího snadný přístup předem sděleny 1) podrobnosti o údajích, které mají být předány; 2) země, do které budou údaje předány (jakož i datum a způsob předání); 3) jméno příjemce a 4) účel použití a uchování příjemcem (čl. 39-12 odst. 3 zákona o ochraně osobních údajů). V takovém případě se kromě toho uplatní i obecné požadavky na zadání činnosti externímu subjektu. Pro každé předání musí být zavedeny zvláštní záruky týkající se zabezpečení, řešení stížností a sporů, jakož i další opatření nezbytná k ochraně údajů uživatelů (článek 48-10 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

([114]) Viz také čl. 26 odst. 7 zákona o ochraně osobních údajů, podle kterého se na zpracovatele obdobně použijí články 15 až 25, 27 až 31, 33 až 38 a 50.

([115]) Pokud poskytovatelé informačních a komunikačních služeb poskytují osobní údaje uživatelů třetí straně, je vždy nutný souhlas uživatele (čl. 39-12 odst. 2 zákona o ochraně osobních údajů).

([116]) Jak je podrobněji vysvětleno v poznámce pod čarou č. 51, aby byl takový souhlas platný, musí být poskytnut svobodně, informovaně a konkrétně.

([117]) Viz také čl. 39-12 odst. 1 zákona o ochraně osobních údajů, pokud jde o poskytovatele informačních a komunikačních služeb.

(89) Bez souhlasu fyzické osoby mohou být osobní údaje poskytnuty třetí straně (v zahraničí), pokud účel zpřístupnění zůstává „v rozsahu přiměřeně souvisejícím“ s původním účelem shromažďování (čl. 17 odst. 4 zákona o ochraně osobních údajů, viz 36. bod odůvodnění). Při rozhodování o tom, zda zpřístupnit (či nezpřístupnit) osobní údaje pro „související“ účel, však musí správce vzít v úvahu, zda zpřístupnění nevede ke znevýhodnění fyzické osoby a zda jsou přijata nezbytná bezpečnostní opatření (např. šifrování). Vzhledem k tomu, že třetí země, do které jsou osobní údaje předávány, nemusí nabízet ochranu obdobnou té, kterou poskytuje zákon o ochraně osobních údajů, oddíl 2 oznámení č. 2021-5 uznává, že k takovým znevýhodněním může dojít a že jim lze předejít pouze tehdy, pokud korejský správce a zahraniční příjemce prostřednictvím právně závazného nástroje (např. smlouvy) zajistí úroveň ochrany srovnatelnou se zákonem o ochraně osobních údajů, a to i s ohledem na práva subjektu údajů.

(90) Zvláštní pravidla platí pro zpřístupnění „za jiným než určeným účelem“, tj. poskytnutí údajů třetí straně za novým (nesouvisejícím) účelem, které se může uskutečnit pouze na základě jednoho z důvodů podle čl. 18 odst. 2 zákona o ochraně osobních údajů, jak je popsáno v 39. bodě odůvodnění. I za těchto podmínek je však poskytnutí údajů třetí straně vyloučeno, pokud je pravděpodobné, že „nekorektním způsobem naruší“ zájmy subjektu údajů nebo třetí strany, což vyžaduje vyvážení zájmů. Kromě toho musí správce podle čl. 18 odst. 5 zákona o ochraně osobních údajů uplatnit další záruky, které mohou zahrnovat požadavek, aby třetí strana omezila účel a způsob zpracování nebo aby zavedla zvláštní bezpečnostní opatření. A opět, vzhledem k tomu, že třetí země, do které jsou osobní údaje předávány, nemusí nabízet ochranu obdobnou té, kterou poskytuje zákon o ochraně osobních údajů, oddíl 2 oznámení č. 2021-5 uznává, že k takovému „nekorektnímu narušení“ zájmů fyzické osoby nebo třetí strany může dojít a lze mu předejít pouze tehdy, pokud korejský správce a zahraniční příjemce prostřednictvím právně závazného nástroje (např. smlouvy) zajistí úroveň ochrany rovnocennou zákonu o ochraně osobních údajů, a to i s ohledem na práva subjektu údajů.

(91) Pravidla v 86. až 90. bodě odůvodnění proto zajišťují kontinuitu ochrany při předání osobních údajů („externímu subjektu zajišťujícímu zpracování“ nebo třetí straně) z Korejské republiky, a to způsobem, který je v zásadě rovnocenný tomu, co stanoví nařízení (EU) 2016/679.

2.3.10 *Odpovědnost*

(92) Podle zásady odpovědnosti se od subjektů zpracovávajících údaje vyžaduje zavedení vhodných technických a organizačních opatření, aby mohly účinně plnit své povinnosti v oblasti ochrany údajů a jejich plnění byly schopny prokázat, zejména příslušnému dozorovému úřadu.

(93) Podle čl. 3 odst. 6 a 8 zákona o ochraně osobních údajů musí správce zpracovávat osobní údaje „způsobem, který minimalizuje možnost narušení“ soukromí subjektu údajů a musí se snažit získat důvěru subjektu údajů dodržováním a plněním úkolů a povinností, jak je stanoví zákon o ochraně osobních údajů a ostatní související právní předpisy. To zahrnuje vytvoření vnitřního plánu řízení (článek 29 zákona o ochraně osobních údajů) a rovněž vhodnou odbornou přípravu zaměstnanců a dohled nad nimi (článek 28 zákona o ochraně osobních údajů).

(94) Jako prostředek zajištění odpovědnosti stanoví článek 31 zákona o ochraně osobních údajů ve spojení s článkem 32 prováděcí vyhlášky k zákonu o ochraně osobních údajů povinnost správců jmenovat pověřence pro ochranu soukromí, který se „komplexně věnuje oblasti zpracování osobních údajů“. Úkolem pověřence pro ochranu soukromí je zejména vykonávat tyto funkce: 1) sestavení a provádění plánu ochrany osobních údajů a vypracování zásad ochrany osobních údajů; 2) provádění pravidelných průzkumů stavu a postupů zpracování osobních údajů s cílem odstranit případné nedostatky; 3) vyřizování stížností a poskytování odškodnění; 4) zřízení vnitřního kontrolního systému, který má zabránit vyzrazení, zneužití a neoprávněnému použití osobních údajů; 5) příprava a realizace vzdělávacího programu; 6) ochrana, kontrola a správa souborů osobních údajů a 7) zničení osobních údajů ihned po dosažení účelu zpracování nebo uplynutí doby uchovávání. Při plnění těchto povinností může pověřenec pro ochranu soukromí kontrolovat stav zpracování osobních údajů a souvisejících systémů a může o tomto zpracování požadovat informace (čl. 31 odst. 3 zákona o ochraně osobních údajů). Pokud pověřenec pro ochranu soukromí zjistí jakékoli porušení zákona o ochraně osobních údajů nebo jiných příslušných právních předpisů v oblasti ochrany údajů, neprodleně přijme nápravná opatření a v případě potřeby tato opatření oznámí vedení („vedoucímu“) správce (čl. 31 odst. 4 zákona o ochraně osobních údajů). Podle čl. 31 odst. 5 zákona o ochraně osobních údajů nesmí být pověřenec pro ochranu soukromí v důsledku výkonu uvedených funkcí bezdůvodně znevýhodňován.

(95) Správci se navíc musí proaktivně snažit provádět posouzení dopadu na soukromí v případě, kdy nakládání se souborem osobních údajů představuje riziko pro soukromí (čl. 33 odst. 8 zákona o ochraně osobních údajů). Na základě čl. 33 odst. 1 a 2 zákona o ochraně osobních údajů ve spojení s články 35, 36 a 38 prováděcí vyhlášky k zákonu o ochraně osobních údajů budou při posuzování míry rizika pro práva subjektů údajů relevantní faktory, jako je druh a povaha zpracovávaných údajů (zejména zda se jedná o citlivé údaje), jejich objem, doba uchovávání a pravděpodobnost porušení zabezpečení údajů. Účelem posouzení dopadu na soukromí je zajistit, aby byly analyzovány rizikové faktory pro soukromí i veškerá bezpečnostní nebo jiná protiopatření, a uvést záležitosti, které vyžadují zlepšení (viz čl. 33 odst. 1 zákona o ochraně osobních údajů ve spojení s článkem 38 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

(96) Veřejné instituce mají povinnost provést posouzení dopadů při zpracování určitých souborů osobních údajů, které představují vyšší riziko možného narušení soukromí (čl. 33 odst. 1 zákona o ochraně osobních údajů). V souladu s článkem 35 prováděcí vyhlášky k zákonu o ochraně osobních údajů se jedná mimo jiné o soubory, které obsahují citlivé údaje týkající se nejméně 50 000 subjektů údajů, soubory, které budou spárovány s jinými soubory, a v důsledku toho budou obsahovat údaje týkající se nejméně alespoň 500 000 subjektů údajů, nebo soubory, které obsahují údaje o alespoň jednom milionu subjektů údajů. Výsledek posouzení dopadů provedeného veřejnou institucí musí být sdělen Komisi pro ochranu osobních údajů (čl. 33 odst. 1 zákona o ochraně osobních údajů), která může vydat stanovisko (čl. 33 odst. 3 zákona o ochraně osobních údajů).

(97) A konečně článek 13 zákona o ochraně osobních údajů uvádí, že Komise pro ochranu osobních údajů stanoví zásady nezbytné k prosazování a podpoře „samoregulačních činností v oblasti ochrany údajů“ ze strany správců, mimo jiné prostřednictvím vzdělávání v oblasti ochrany údajů, prosazování a podpory organizací činných v oblasti ochrany údajů a prostřednictvím pomoci poskytované správcům při zavádění a provádění samoregulačních pravidel. Kromě toho komise zavede a usnadní systém známky ochrany soukromí v oblasti elektronických komunikací, tzv. ePRIVACY. V tomto ohledu článek 32-2 zákona o ochraně osobních údajů ve spojení s články 34-2 až 34-8 prováděcí vyhlášky k zákonu o ochraně osobních údajů nabízí možnost certifikovat, že systémy zpracování a ochrany osobních údajů správce splňují požadavky zákona o ochraně osobních údajů. Podle těchto pravidel může být certifikace ([118]) udělena (na dobu tří let), pokud správce splní certifikační kritéria stanovená Komisí pro ochranu osobních údajů, včetně zavedení řídicích, technických a fyzických záruk ochrany osobních údajů ([119]). Aby byla zachována účinnost certifikace, musí Komise pro ochranu osobních údajů prověřit systémy správce relevantní pro certifikaci alespoň jednou ročně, což může vést ke zrušení certifikace (čl. 32 odst. 4 zákona o ochraně osobních údajů ve spojení s článkem 34-5 prováděcí vyhlášky k zákonu o ochraně osobních údajů; tzv. „následná správa“).

(98) Korejský rámec proto zavádí zásadu odpovědnosti způsobem, který zajišťuje úroveň ochrany v zásadě rovnocennou ochraně podle nařízení (EU) 2016/679, a to i stanovením různých mechanismů k zajištění a prokázání souladu se zákonem o ochraně osobních údajů.

2.3.11 *Zvláštní pravidla pro zpracování osobních úvěrových informací*

(99) Jak je popsáno v 13. bodě odůvodnění, zákon o používání a ochraně úvěrových informací stanoví zvláštní pravidla pro zpracování osobních úvěrových informací komerčními hospodářskými subjekty. Při zpracování osobních úvěrových informací proto musí komerční hospodářské subjekty dodržovat obecné požadavky zákona o ochraně osobních údajů, pokud zákon o používání a ochraně úvěrových informací neobsahuje konkrétnější pravidla. Bude tomu tak například v případě, kdy komerční hospodářské subjekty zpracovávají informace týkající se kreditní karty nebo bankovního účtu v rámci obchodní transakce s fyzickou osobou. Jako odvětvový právní předpis pro zpracování úvěrových informací (osobních i neosobních) zákon o používání a ochraně úvěrových informací nejen ukládá zvláštní záruky ochrany údajů (například pokud jde o transparentnost a bezpečnost), ale také obecněji upravuje konkrétní okolnosti, za nichž lze osobní úvěrové informace zpracovávat. To se odráží zejména v podrobných požadavcích na používání údajů, poskytování údajů třetí straně a uchovávání těchto údajů.

(100) Stejně jako zákon o ochraně osobních údajů i zákon o používání a ochraně úvěrových informací odráží zásadu zákonnosti a proporcionality. Zaprvé čl. 15 odst. 1 zákona o používání a ochraně úvěrových informací obecně povoluje shromažďování osobních úvěrových informací pouze přiměřenými a korektními prostředky a v minimálním rozsahu nezbytném k naplnění stanoveného účelu v souladu s čl. 3 odst. 1 a 2 zákona o ochraně osobních údajů. Zadruhé zákon o používání a ochraně úvěrových informací konkrétně upravuje zákonnost zpracování osobních úvěrových informací tím, že omezuje jejich shromažďování, používání a poskytování třetí straně a obecně váže tyto činnosti zpracování na povinnost získat souhlas dotčené osoby.

([118]) Pokud navíc správce hodlá odkazovat na certifikaci nebo ji propagovat v rámci svých obchodních operací, může použít označení ochrany osobních údajů, které zavedla Komise pro ochranu osobních údajů. Viz článek 34-7 prováděcí vyhlášky k zákonu o ochraně osobních údajů.

([119]) Od listopadu 2018 byl vyvíjen „Systém správy zabezpečení osobních údajů a informací“ (Personal Information & Information Security Management System, ISMS-P), který osvědčuje, že správci provozují komplexní systém správy.

(101) Osobní úvěrové informace mohou být shromažďovány na základě jednoho z důvodů stanovených v zákoně o ochraně osobních údajů nebo konkrétních důvodů stanovených v zákoně o používání a ochraně úvěrových informací. Vzhledem k tomu, že článek 45 nařízení (EU) 2016/679 předpokládá předání osobních údajů správcem nebo zpracovatelem v Unii, ale nezahrnuje přímé shromažďování (například od fyzické osoby nebo z internetových stránek) správcem v Koreji, jsou pro toto rozhodnutí relevantní pouze souhlas a důvody podle zákona o ochraně osobních údajů. K těmto důvodům patří zejména situace, kdy je předání nezbytné pro plnění smlouvy s fyzickou osobou nebo pro oprávněné zájmy korejského správce (čl. 15 odst. 1 body 4 a 6 zákona o ochraně osobních údajů) ([120]).

(102) Po jejich shromáždění mohou být osobní úvěrové informace použity 1) pro původní účel, pro který byly (přímo) poskytnuty fyzickou osobou ([121]); 2) pro účel slučitelný s původním účelem shromažďování ([122]); 3) k určení toho, zda navázat nebo udržet obchodní vztah požadovaný fyzickou osobou ([123]); 4) pro účely statistiky, výzkumu a archivace ve veřejném zájmu ([124]), jsou-li informace pseudonymizované ([125]); 5) pokud je získán další souhlas, nebo 6) v souladu se zákonem.

(103) Pokud komerční hospodářský subjekt hodlá sdělit osobní úvěrové informace třetí straně, musí získat souhlas dané fyzické osoby ([126]) poté, co jí sdělí příjemce údajů, účel zpracování příjemcem, podrobnosti údajů, které mají být poskytnuty, dobu uchovávání příjemcem a právo odmítnout souhlas (čl. 32 odst. 1 zákona o používání a ochraně úvěrových informací a čl. 28 odst. 2 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací) ([127]). Tento požadavek souhlasu se nepoužije v konkrétních situacích, jmenovitě pokud jsou osobní úvěrové informace zpřístupněny ([128]): 1) externímu subjektu zajišťujícímu zpracování pro účely tohoto externího zpracování ([129]); 2) třetí straně v případě převodu, rozdělení nebo fúze podniku; 3) pro účely statistiky, výzkumu a archivace ve veřejném zájmu, jsou-li informace pseudonymizované; 4) pro účel slučitelný s původním účelem shromažďování; 5) třetí straně, která používá informace k vymáhání dluhu fyzické osoby ([130]); 6) pro splnění

([120]) Zákon o používání a ochraně úvěrových informací obsahuje i další právní základy shromažďování, tzn. případy, kdy je vyžaduje zákon, kdy informace zveřejňuje veřejná instituce podle právních předpisů v oblasti svobody informací nebo kdy jsou informace dostupné na sociální síti. Aby se komerční hospodářský subjekt mohl opřít o poslední důvod, musí být schopen prokázat, že shromažďování zůstává v mezích souhlasu subjektu údajů, a to na základě přiměřeného („objektivního“) výkladu a s přihlédnutím k povaze údajů, záměru a účelu jejich zpřístupnění na sociální síti a k tomu, zda je účel shromažďování pro tento účel „vysoce relevantní“ atd. (článek 13 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací). Jak je však vysvětleno ve 101. bodě odůvodnění, tyto důvody v zásadě nebudou v situaci předání relevantní.

([121]) Například když jsou úvěrové informace generovány/poskytovány v souvislosti s obchodní transakcí s fyzickou osobou. O tento důvod se však nelze opřít při použití osobních úvěrových informací pro účely přímého marketingu (viz čl. 33 odst. 1 bod 3 zákona o používání a ochraně úvěrových informací).

([122]) Pro určení toho, zda je účel použití slučitelný s původním účelem shromažďování, je třeba vzít v úvahu tyto faktory: 1) vztah („relevanci“) obou účelů; 2) způsob, jakým byly informace shromážděny; 3) dopad použití na fyzickou osobu a 4) zda byla přijata vhodná bezpečnostní opatření, například pseudonymizace (srov. čl. 32 odst. 6 bod 9-4 zákona o používání a ochraně úvěrových informací).

([123]) Správce musí například zohlednit osobní úvěrové informace, které obdržel od fyzické osoby, aby se mohl rozhodnout, zda této fyzické osobě prodlouží dobu trvání půjčky.

([124]) Článek 33 zákona o používání a ochraně úvěrových informací ve spojení s čl. 32 odst. 6 body 9-2 a 9-4 a 10 zákona o používání a ochraně úvěrových informací.

([125]) Pseudonymizace je v čl. 2 odst. 15 zákona o používání a ochraně úvěrových informací definována jako zpracování osobních úvěrových informací takovým způsobem, že fyzickou osobu již nelze z těchto informací identifikovat jinak než v kombinaci s dalšími údaji. Přestože zákon o používání a ochraně úvěrových informací obsahuje zvláštní záruky pro zpracování pseudonymizovaných údajů pro účely statistiky, výzkumu a archivace ve veřejném zájmu (článek 40-2 zákona o používání a ochraně úvěrových informací), tato pravidla se nevztahují na komerční organizace. Namísto toho se na tyto organizace nadále vztahují zvláštní požadavky oddílu III zákona o ochraně osobních údajů, jak je popsáno ve 42. až 48. bodě odůvodnění. Článek 40-3 zákona o používání a ochraně úvěrových informací dále vyjímá zpracování pseudonymizovaných úvěrových informací (pokud je prováděno pro účely statistiky, vědeckého výzkumu nebo archivace ve veřejném zájmu) z požadavků na transparentnost a individuální práva, podobně jako v případě výjimky v článku 28-7 zákona o ochraně osobních údajů a s výhradou záruk podle oddílu III zákona o ochraně osobních údajů, jak je podrobněji popsáno ve 42. až 48. bodě odůvodnění.

([126]) Toto ustanovení se nepoužije, pokud jsou informace poskytovány třetí straně s cílem zajistit, aby byly osobní úvěrové informace přesné a aktuální, pokud poskytnutí zůstává v mezích původního účelu zpracování (čl. 32 odst. 1 zákona o používání a ochraně úvěrových informací). K tomu může dojít například v případě, že jsou ratingové agentuře poskytnuty aktuální informace, aby byla zajištěna přesnost jejích záznamů.

([127]) Není-li možné výše uvedené informace poskytnout, může být dostačující odkázat fyzickou osobu ve věci požadovaných informací na přijímající třetí stranu.

([128]) Vzhledem k tomu, že zákon o používání a ochraně úvěrových informací výslovně neupravuje zahraniční zpřístupňování osobních úvěrových informací, musí takové zpřístupnění splňovat záruky pro další předávání uložené oddílem 2 oznámení č. 2021-5.

([129]) Zadání externího zpracování osobních úvěrových informací může probíhat pouze na základě písemné smlouvy a v souladu s požadavky čl. 26 odst. 1 až 3 a 5 zákona o ochraně osobních údajů, jak je popsáno ve 20. bodě odůvodnění (článek 17 zákona o používání a ochraně úvěrových informací a článek 14 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací). Externí subjekt zajišťující zpracování nesmí používat informace nad rámec povinností zadaných k externímu zajištění a společnost, která zadává externí zpracování, musí zavést zvláštní bezpečnostní požadavky (např. šifrování) a poučit externí subjekt zajišťující zpracování o tom, jak zabránit ztrátě, odcizení, zpřístupnění, změně nebo vyzrazení úvěrových informací.

([130]) Viz také čl. 28 odst. 10 bod 1, 2 a 6 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací.

soudního příkazu; 7) státnímu zástupci / příslušníkovi soudní policie v případě nouze, kdy je fyzická osoba ohrožena na životě nebo se očekává, že utrpí újmu na zdraví a není čas na vydání soudního příkazu ([131]); 8) příslušným daňovým orgánům pro účely dodržování daňových zákonů, nebo 9) v souladu s jinými zákony. V případě zpřístupnění na základě jednoho z těchto důvodů o tom musí být subjekt údajů předem informován (čl. 32 odst. 7 zákona o používání a ochraně úvěrových informací).

(104) Zákon o používání a ochraně úvěrových informací také konkrétně upravuje dobu zpracování osobních úvěrových informací na základě jednoho z uvedených důvodů pro účely použití nebo poskytnutí třetí straně po skončení obchodního vztahu s fyzickou osobou ([132]). Mohou být uchovány pouze informace, které byly nezbytné k navázání nebo udržení tohoto vztahu, s výhradou dalších záruk (musí být uchovávány odděleně od úvěrových informací, které se týkají fyzických osob, s nimiž existuje obchodní vztah, musí být chráněny zvláštními bezpečnostními opatřeními a musí být přístupné pouze oprávněným fyzickým osobám) ([133]). Všechny ostatní údaje musí být vymazány (čl. 17-2 odst. 1 bod 2 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací). Při určení toho, které údaje byly nezbytné pro obchodní vztah, je třeba vzít v úvahu různé faktory, včetně toho, zda by bylo možné navázat vztah bez těchto údajů a zda se údaje přímo týkají zboží nebo služeb poskytovaných dané fyzické osobě (čl. 17-2 odst. 2 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací).

(105) I v případech, kdy mohou být osobní úvěrové informace v zásadě uchovávány i po skončení obchodního vztahu, musí být vymazány do tří měsíců po dosažení dalšího účelu zpracování ([134]) nebo v každém případě po pěti letech (článek 20-2 zákona o používání a ochraně úvěrových informací). V omezeném počtu situací lze osobní úvěrové informace uchovávat déle než pět let, zejména je-li to nezbytné pro splnění zákonné povinnosti; je-li to nezbytné pro životně důležité zájmy týkající se života, zdraví nebo majetku jednotlivce; pro archivaci pseudonymizovaných údajů (které byly použity pro účely vědeckého výzkumu, statistiky nebo archivace ve veřejném zájmu), nebo pro účely pojištění (zejména pro platby pojistného nebo pro předcházení pojistným podvodům) ([135]). V těchto výjimečných případech se použijí zvláštní záruky (jako je oznámení fyzické osobě o dalším použití, oddělení uchovávaných informací od informací, které se týkají fyzických osob, s nimiž stále existuje obchodní vztah, omezení přístupových práv, viz čl. 17-2 odst. 1 a 2 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací).

(106) Zákon o používání a ochraně úvěrových informací rovněž dále specifikuje zásady přesnosti a kvality údajů, neboť požaduje, aby osobní úvěrové informace byly „registrovány, upravovány a spravovány“ s cílem udržovat jejich přesnost a aktuálnost (čl. 18 odst. 1 zákona o používání a ochraně úvěrových informací a čl. 15 odst. 3 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací) ([136]). Při poskytování úvěrových informací určitým dalším subjektům (například ratingovým agenturám) se od komerčních hospodářských subjektů také výslovně požaduje, aby ověřily přesnost informací a zajistily tak, že příjemce zaregistruje a bude spravovat pouze přesné informace (čl. 15 odst. 1 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací ve spojení s čl. 18 odst. 1 zákona o používání a ochraně úvěrových informací). Obecněji řečeno, zákon o používání a ochraně úvěrových informací vyžaduje, aby byly vedeny záznamy o shromažďování, používání, zpřístupňování třetím stranám a ničení osobních úvěrových informací (čl. 20 odst. 2 zákona o používání a ochraně úvěrových informací) ([137]).

(107) Kromě toho zpracování osobních úvěrových informací podléhá zvláštním požadavkům v oblasti zabezpečení údajů. Zákon o používání a ochraně úvěrových informací zejména vyžaduje provedení technických, fyzických a organizačních opatření, která mají zabránit nezákonnému přístupu k počítačovým systémům, jakož i změně, zničení nebo jinému riziku pro zpracovávané údaje (například prostřednictvím kontroly přístupu, viz článek 19 zákona o používání a ochraně úvěrových informací a článek 16 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací o prosazování). Kromě toho musí být při výměně osobních úvěrových informací s třetí stranou uzavřena dohoda, která stanoví konkrétní bezpečnostní opatření (čl. 19 odst. 2 zákona o používání a ochraně úvěrových informací). Pokud dojde k porušení zabezpečení osobních úvěrových informací, musí být přijata opatření k minimalizaci jakýchkoli škod a musí být neprodleně vyrozuměny dotčené fyzické osoby (čl. 39-4 odst. 1 a 2 zákona o používání a ochraně úvěrových informací). Kromě toho musí být Komise pro ochranu osobních údajů informována o oznámení poskytnutém fyzickým osobám a o opatřeních, která byla provedena (čl. 39-4 odst. 4 zákona o používání a ochraně úvěrových informací).

([131]) V takovém případě je třeba neprodleně požádat o soudní příkaz. Není-li příkaz vydán do 36 hodin, musí být přijaté údaje neprodleně vymazány (čl. 32 odst. 6 bod 6 zákona o používání a ochraně úvěrových informací).

([132]) Například z toho důvodu, že byly splněny smluvní závazky, jedna ze stran uplatnila své právo na ukončení smlouvy atd., viz čl. 17-2 odst. 5 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací.

([133]) Ustanovení čl. 20-2 odst. 1 zákona o používání a ochraně úvěrových informací a čl. 17-2 odst. 1 bod 1 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací.

([134]) Tato lhůta zohledňuje skutečnost, že výmaz často nelze provést okamžitě, ale obvykle vyžaduje určité kroky, jejichž provedení trvá určitou dobu (např. oddělení údajů, které mají být vymazány, od ostatních dat a provedení výmazu bez ovlivnění stability informačních systémů).

([135]) Ustanovení čl. 20-2 odst. 2 zákona o používání a ochraně úvěrových informací.

([136]) Ustanovení čl. 18 odst. 2 zákona o používání a ochraně úvěrových informací a čl. 15 odst. 4 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací stanoví konkrétnější pravidla týkající se tohoto požadavku vedení záznamů, např. pro záznamy týkající se informací, které mohou fyzickou osobu znevýhodnit, jako jsou informace o nesplácení a úpadku.

([137]) Pokud jde o další mechanismy odpovědnosti, zákon o používání a ochraně úvěrových informací vyžaduje, aby určité organizace (např. družstva a veřejné korporace, viz čl. 21 odst. 2 vyhlášky o prosazování zákona o používání a ochraně úvěrových informací) jmenovaly „správce/zástupce pro úvěrové informace“, který odpovídá za sledování toho, jak je dodržován zákon o používání a ochraně úvěrových informací, a plní úkoly „pověřence pro ochranu soukromí“ podle zákona o ochraně osobních údajů (čl. 20 odst. 3 a 4 zákona o používání a ochraně úvěrových informací).

(108) Zákon o používání a ochraně úvěrových informací rovněž ukládá specifické povinnosti týkající se transparentnosti při získávání souhlasu s používáním nebo poskytováním osobních úvěrových informací (čl. 32 odst. 4 a čl. 34-2 zákona o používání a ochraně úvěrových informací a článek 30-3 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací) a obecněji před poskytnutím informací třetí straně (čl. 32 odst. 7 zákona o používání a ochraně úvěrových informací) ([138]). Kromě toho mají fyzické osoby právo na vyžádání obdržet informace o použití a poskytnutí jejich úvěrových informací třetím stranám během tří let předcházejících žádosti (včetně účelu a dat takového použití/poskytnutí) ([139]).

(109) Podle zákona o používání a ochraně úvěrových informací mají fyzické osoby také právo na přístup ke svým osobním úvěrovým informacím (čl. 38 odst. 1 zákona o používání a ochraně úvěrových informací) a právo na opravu nepřesných údajů (čl. 38 odst. 2 a 3 zákona o používání a ochraně úvěrových informací) ([140]). Navíc kromě obecného práva na výmaz podle zákona o ochraně osobních údajů (viz 77. bod odůvodnění) zákon o používání a ochraně úvěrových informací stanoví zvláštní právo na výmaz osobních úvěrových informací, které jsou uchovávány po dobu uchovávání uvedenou ve 104. bodě odůvodnění, tj. po dobu pěti let (u osobních úvěrových informací, které byly nezbytné k navázání nebo udržení obchodního vztahu) nebo tří měsíců (u jiných druhů osobních úvěrových informací) ([141]). Žádost o výmaz může být výjimečně zamítnuta, pokud je další uchovávání nezbytné v situaci popsané ve 105. bodě odůvodnění. Pokud fyzická osoba požaduje výmaz, ale použije se jedna z výjimek, musí být u dotčených úvěrových informací uplatněny zvláštní záruky (článek 38-3 odst. 3 zákona o používání a ochraně úvěrových informací a článek 33-3 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací). Informace musí být například uchovávány odděleně od ostatních informací, může k nim mít přístup pouze oprávněná osoba a musí podléhat zvláštním bezpečnostním opatřením.

(110) Vedle práv uvedených ve 109. bodě odůvodnění zaručuje zákon o používání a ochraně úvěrových informací fyzickým osobám právo požádat správce, aby je přestal kontaktovat pro účely přímého marketingu (čl. 37 odst. 2 zákona) a právo na přenositelnost údajů. Pokud jde o posledně uvedené právo, zákon o používání a ochraně úvěrových informací umožňuje fyzickým osobám požádat, aby byly jejich osobní úvěrové informace předány jim samotným, nebo určitým třetím stranám (například finančním institucím a ratingovým společnostem). Osobní úvěrové informace musí být zpracovány a předány třetí straně ve formátu, který lze zpracovat zařízením pro zpracování informací (například počítačem).

(111) Pokud jde o to, že zákon o používání a ochraně úvěrových informací obsahuje oproti zákonu o ochraně osobních údajů specifická pravidla, komise má za to, že i tato pravidla zajišťují úroveň ochrany v zásadě rovnocennou úrovni ochrany, kterou poskytuje nařízení (EU) 2016/679.

2.4 **Dozor a vymáhání**

(112) Aby se zajistilo, že odpovídající úroveň ochrany údajů je zaručena v praxi, měl by být zřízen nezávislý dozorový úřad oprávněný monitorovat a vymáhat dodržování pravidel v oblasti ochrany údajů. Při plnění svých povinností a výkonu své pravomoci by tento úřad měl jednat zcela nezávisle a nestranně.

2.4.1 *Nezávislý dozor*

(113) V Korejské republice je orgánem pověřeným monitorovat a prosazovat zákon o ochraně osobních údajů Komise pro ochranu osobních údajů. Komise pro ochranu osobních údajů se skládá z předsedy, místopředsedy a sedmi komisařů. Předsedu a místopředsedu jmenuje prezident na návrh předsedy vlády. Dva komisaře jmenuje prezident

([138]) To zahrnuje obecnou oznamovací povinnost (čl. 32 odst. 7 zákona o používání a ochraně úvěrových informací) a specifickou povinnost transparentnosti v případě, že jsou informace, na jejichž základě lze určit úvěruschopnost fyzické osoby, poskytnuty určitým subjektům, jako jsou ratingové agentury a agentury pro shromažďování úvěrových informací (článek 35-3 zákona o používání a ochraně úvěrových informací a článek 30-3 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací), nebo pokud je obchodní transakční vztah odmítnut nebo ukončen na základě osobních úvěrových informací obdržených od třetí strany (článek 36 zákona o používání a ochraně úvěrových informací a článek 31 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací).

([139]) Článek 35 zákona o používání a ochraně úvěrových informací. Určité komerční organizace, např. družstva a veřejné korporace (viz čl. 21 odst. 2 vyhlášky o prosazování zákona o používání a ochraně úvěrových informací), podléhají dalším požadavkům na transparentnost, např. povinnosti zpřístupnit určité informace veřejnosti (článek 31 zákona o používání a ochraně úvěrových informací) a informovat fyzické osoby o možných znevýhodněních pro jejich úvěrový rating při zapojení do finančních transakcí, které představují úvěrová rizika (článek 35-2 zákona o používání a ochraně úvěrových informací).

([140]) Pokud jde o podmínky a výjimky z práv na přístup a opravu, použijí se pravidla zákona o ochraně osobních údajů (popsaná v 76. a 77. bodě odůvodnění). Další možnosti dále stanoví čl. 38 odst. 4 až 8 zákona o používání a ochraně úvěrových informací a článek 33 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací. Konkrétně komerční hospodářský subjekt, který opravil nebo vymazal nepřesné úvěrové informace, musí o výmazu informovat danou fyzickou osobu. Kromě toho musí být informována jakákoli třetí strana, které byly tyto informace zpřístupněny během předchozích šesti měsíců, a dotčená fyzická osoba o tom musí být vyrozuměna. Pokud fyzická osoba není spokojena s tím, jak byla vyřízena její žádost o opravu, může předložit žádost Komisi pro ochranu osobních údajů, která ověří kroky správce a může uložit nápravná opatření.

([141]) Článek 38-3 zákona o používání a ochraně úvěrových informací.

na návrh předsedy a pět na návrh Národního shromáždění (z nich dva na návrh politické strany, k níž náleží prezident, a tři na návrh jiných politických stran (čl. 7-2 odst. 2 zákona o ochraně osobních údajů), což pomáhá odstranit stranickost v procesu jmenování) ([142]). Tento postup je v souladu s podmínkami jmenování členů úřadů pro ochranu údajů v Unii (čl. 53 odst. 1 nařízení (EU) 2016/679). Kromě toho se všichni komisaři musí zdržet jakýchkoli obchodních činností za účelem zisku a politických aktivit a nesmí zastávat funkce ve veřejné správě nebo v Národním shromáždění (článek 7-6 a čl. 7-7 odst. 1 bod 3 zákona o ochraně osobních údajů) ([143]). Na všechny komisaře se vztahují také zvláštní pravidla, která jim brání v účasti na rozhodování v případě možného střetu zájmů (článek 7-11 zákona o ochraně osobních údajů). Komisi pro ochranu osobních údajů je nápomocen sekretariát (články 7-13) a Komise může zřizovat podkomise (složené ze tří komisařů) pro řešení menších porušení a častých záležitostí (článek 7-12 zákona o ochraně osobních údajů).

(114) Každý člen Komise pro ochranu osobních údajů je jmenován na tři roky a může být jednou opětovně jmenován (čl. 7-4 odst. 1 zákona o ochraně osobních údajů). Komisaři mohou být odvoláni pouze za zvláštních okolností, zejména pokud již nemohou vykonávat svou funkci z důvodu dlouhodobého mentálního nebo tělesného postižení, jednají v rozporu se zákonem nebo naplňují některý z důvodů nezpůsobilosti pro výkon funkce ([144]) (článek 7-5 zákona o ochraně osobních údajů). To jim poskytuje institucionální ochranu při výkonu jejich funkcí.

(115) V obecnějším smyslu čl. 7 odst. 1 zákona o ochraně osobních údajů výslovně zaručuje nezávislost Komise pro ochranu osobních údajů a čl. 7-5 odst. 2 zákona o ochraně osobních údajů vyžaduje, aby komisaři vykonávali své povinnosti nezávisle, v souladu se zákonem a svým svědomím ([145]). Popsané institucionální a procesní záruky včetně těch, které se týkají jmenování a odvolání jejích členů, zajišťují, že Komise pro ochranu osobních údajů jedná zcela nezávisle, bez vnějšího vlivu a nepodléhá žádným pokynům. Komise pro ochranu osobních údajů dále jakožto ústřední správní úřad každoročně navrhuje svůj rozpočet (který před schválením Národním shromážděním přezkoumává ministerstvo financí v rámci celkového státního rozpočtu) a odpovídá za své personální řízení. V současnosti disponuje Komise pro ochranu osobních údajů rozpočtem přibližně 35 milionů EUR a má 154 zaměstnanců (včetně 40 specialistů na informační a komunikační technologie, 32 zaměstnanců zaměřených na vyšetřování a 40 právních odborníků).

(116) Úkoly a pravomoci Komise pro ochranu osobních údajů stanoví zejména články 7-8 a 7-9, jakož i články 61 až 66 zákona o ochraně osobních údajů ([146]). Úkoly a pravomoci Komise pro ochranu osobních údajů zahrnují zejména poradenství v oblasti právních a správních předpisů souvisejících s ochranou údajů, tvorbu zásad a pokynů v oblasti ochrany údajů, vyšetřování případů porušení individuálních práv, vyřizování stížností a mediaci ve sporech, vymáhání dodržování zákona o ochraně osobních údajů, zajišťování vzdělávání a propagace v oblasti ochrany údajů a výměny a spolupráce s úřady pro ochranu údajů v třetích zemích ([147]).

(117) Na základě článku 68 zákona o ochraně osobních údajů ve spojení s článkem 62 prováděcí vyhlášky k zákonu o ochraně osobních údajů byly některé úkoly Komise pro ochranu osobních údajů delegovány na Korejskou agenturu pro internet a bezpečnost, a to konkrétně: 1) vzdělávání a styk s veřejností; 2) školení specialistů a vývoj kritérií pro posuzování dopadů na soukromí; 3) vyřizování žádostí o určení tzv. instituce pro posuzování vlivů na soukromí; 4) vyřizování žádostí o nepřímý přístup k osobním údajům drženým orgány veřejné správy

([142]) Členy Komise pro ochranu osobních údajů mohou být jmenovány pouze osoby splňující tato kritéria: vyšší státní úředníci odpovědní za záležitosti týkající se osobních údajů; bývalí soudci, státní zástupci nebo advokáti s nejméně desetiletou praxí; bývalí vedoucí pracovníci s praxí v oblasti ochrany údajů, kteří pracovali ve veřejné instituci nebo organizaci déle než tři roky nebo byli takovou institucí nebo organizací doporučeni, a bývalí docenti s odbornými znalostmi v oblasti ochrany údajů, kteří působili po dobu nejméně pěti let v akademické instituci (článek 7-2 zákona o ochraně osobních údajů).

([143]) Viz také článek 4-2 prováděcí vyhlášky k zákonu o ochraně osobních údajů.

([144]) Viz článek 7-7 zákona o ochraně osobních údajů, podle kterého se členy Komise pro ochranu osobních údajů nemohou stát cizí státní příslušníci a členové politických stran. Totéž platí pro fyzické osoby, kterým byly uloženy určité druhy trestních sankcí, byly v posledních pěti letech zbaveny funkce v disciplinárním řízení atd. (článek 7-7 zákona o ochraně osobních údajů ve spojení s článkem 33 zákona o státních úřednících).

([145]) Zatímco čl. 7 odst. 2 zákona o ochraně osobních údajů odkazuje na obecnou pravomoc předsedy vlády podle článku 18 zákona o organizaci vlády pozastavit nebo zrušit (se souhlasem prezidenta) jakékoli nezákonné nebo nekorektní opatření ústředního správního úřadu, žádná taková pravomoc není udělena, pokud jde o vyšetřovací nebo donucovací pravomoci Komise pro ochranu osobních údajů (viz čl. 7 odst. 2 body 1 a 2 zákona o ochraně osobních údajů). Podle vysvětlení obdržených od korejské vlády má článek 18 zákona o organizaci vlády poskytnout předsedovi vlády možnost jednat za mimořádných okolností, např. mediačně řešit neshody mezi různými vládními úřady. Od přijetí tohoto ustanovení v roce 1963 však premiér tuto pravomoc nikdy nevyužil.

([146]) Je-li to nezbytné k plnění úkolů podle čl. 7-9 odst. 1 zákona o ochraně osobních údajů, může si Komise pro ochranu osobních údajů vyžádat stanoviska příslušných státních úředníků, odborníků v oblasti ochrany údajů, občanských organizací a relevantních podnikatelských subjektů. Kromě toho si Komise pro ochranu osobních údajů může vyžádat příslušné materiály, vydávat doporučení ke zlepšení a kontrolovat, zda jsou prováděna (čl. 7-9 odst. 2 až 5 zákona o ochraně osobních údajů).

([147]) Viz také článek 9 zákona o ochraně osobních údajů (tříletý základní plán ochrany osobních údajů), článek 12 zákona o ochraně osobních údajů (standardní pokyny pro ochranu osobních údajů), článek 13 zákona o ochraně osobních údajů (zásady prosazování a podpory samoregulace).

(čl. 35 odst. 2 zákona o ochraně osobních údajů) a 5) vyžadování materiálů a provádění kontrol týkajících se stížností obdržených prostřednictvím tzv. kontaktního centra pro ochranu soukromí. V rámci vyřizování stížností prostřednictvím kontaktního centra pro ochranu soukromí Korejská agentura pro internet a bezpečnost postoupí věc Komisi pro ochranu osobních údajů nebo státnímu zastupitelství, pokud zjistí, že došlo k porušení zákona. Možnost podat stížnost kontaktnímu centru pro ochranu soukromí nebrání fyzickým osobám podat stížnost přímo Komisi pro ochranu osobních údajů nebo se na Komisi pro ochranu osobních údajů obrátit, pokud se domnívají, že jejich stížnost nebyla Korejskou agenturou pro internet a bezpečnost uspokojivě vyřízena.

2.4.2 *Vymáhání včetně sankcí*

(118) S cílem zajistit soulad se zákonem o ochraně osobních údajů zákonodárce udělil Komisi pro ochranu osobních údajů vyšetřovací i donucovací pravomoci sahající od doporučení až po správní pokuty. Tyto pravomoci dále doplňuje režim trestních sankcí.

(119) Pokud jde o vyšetřovací pravomoci, existuje-li podezření na porušení zákona o ochraně osobních údajů nebo bylo takové porušení oznámeno nebo je-li to nezbytné pro ochranu práv subjektu údajů před porušením, může Komise pro ochranu osobních údajů provádět kontroly na místě a vyžádat si všechny relevantní materiály (například věci a dokumenty) od správců osobních údajů (článek 63 zákona o ochraně osobních údajů ve spojení s článkem 60 prováděcí vyhlášky k zákonu o ochraně osobních údajů) ([148]).

(120) Pokud jde o prosazování, podle čl. 61 odst. 2 zákona o ochraně osobních údajů může Komise pro ochranu osobních údajů poskytovat správcům údajů poradenství, jak zlepšit úroveň ochrany osobních údajů u konkrétních činností zpracování. Správci údajů musí v dobré víře vynaložit úsilí na provedení takového poradenství a jsou povinni o výsledku informovat Komisi pro ochranu osobních údajů. Pokud navíc existují rozumné důvody se domnívat, že došlo k porušení zákona o ochraně osobních údajů a nečinnost pravděpodobně způsobí těžko napravitelnou škodu, může Komise pro ochranu osobních údajů uložit nápravná opatření (čl. 64 odst. 1 zákona o ochraně osobních údajů) ([149]). Oddíl 5 oznámení č. 2021-5 (příloha I) vysvětluje, a to se závazným účinkem, že tyto podmínky jsou splněny ve vztahu k porušení kteréhokoli ustanovení zákona o ochraně osobních údajů, které chrání práva fyzických osob na soukromí, pokud jde o osobní údaje ([150]). Opatření, která je Komise pro ochranu osobních údajů oprávněna přijmout, zahrnují příkaz k zastavení jednání způsobujícího porušení, dočasné pozastavení zpracování údajů nebo jakákoli jiná nezbytná opatření. Nedodržení nápravného opatření může vést k sankci v podobě pokuty až do výše 50 milionů wonů (čl. 75 odst. 2 bod 13 zákona o ochraně osobních údajů).

(121) Pokud jde o některé orgány veřejné správy (např. Národní shromáždění, ústřední správní agentury, orgány místní správy a soudy), čl. 64 odst. 4 zákona o ochraně osobních údajů stanoví, že Komise pro ochranu osobních údajů může „doporučit" jakákoli nápravná opatření uvedená ve 120. bodě odůvodnění a že tyto orgány jsou povinny se takovým doporučením řídit, nenastanou-li mimořádné okolnosti. Podle oddílu 5 oznámení č. 2021-5 se to týká mimořádných skutkových nebo právních okolností, kterých si Komise pro ochranu osobních údajů při vydávání doporučení nebyla vědoma. Dotčený orgán veřejné správy se může na takové mimořádné okolnosti odvolat pouze tehdy, pokud jasně prokáže, že k žádnému porušení nedošlo, a Komise pro ochranu osobních údajů rozhodne, že tomu tak skutečně nebylo. V opačném případě se orgán veřejné správy musí řídit doporučením Komise pro ochranu osobních údajů a „přijmout nápravná opatření, včetně okamžitého zastavení jednání a náhrady škody ve výjimečném případě, kdy byl nezákonný čin přesto spáchán".

(122) Komise pro ochranu osobních údajů může rovněž požádat jiné správní úřady, jimž odvětvové právní předpisy svěřují specifické pravomoci (např. ve zdravotnictví, vzdělávání), aby samy nebo společně s ní provedly vyšetřování (podezření na) porušení soukromí ze strany správců údajů působících v těchto odvětvích spadajících do jejich jurisdikce a uložily nápravná opatření (čl. 63 odst. 4 a 5 zákona o ochraně osobních údajů). V takovém případě Komise pro ochranu osobních údajů určí důvody, předmět a rozsah vyšetřování ([151]). Příslušný správní úřad pak musí Komisi pro ochranu osobních údajů předložit plán inspekce a oznámit jí výsledek této inspekce. Komise pro ochranu osobních údajů může doporučit přijetí specifického nápravného opatření a příslušný úřad se musí snažit o jeho zavedení. V každém případě taková žádost neomezuje pravomoc Komise pro ochranu osobních údajů provádět vlastní vyšetřování nebo ukládat sankce.

([148]) Komise pro ochranu osobních údajů může dále vstoupit do prostor správce za účelem kontroly stavu obchodních operací, záznamů, dokumentů atd. (čl. 63 odst. 2 zákona o ochraně osobních údajů). Viz také článek 45-3 zákona o používání a ochraně úvěrových informací a článek 36-4 prováděcí vyhlášky k zákonu o používání a ochraně úvěrových informací, pokud jde o pravomoci Komise pro ochranu osobních údajů podle uvedeného zákona.

([149]) Pravomoci Komise pro ochranu osobních údajů podle zákona o používání a ochraně úvěrových informací viz také článek 45-4 uvedeného zákona.

([150]) Oddíl 5 oznámení stanoví, že „závažný důvod se domnívat, že došlo k porušení předpisů v oblasti osobních údajů a nečinnost pravděpodobně způsobí obtížně napravitelnou škodu ve smyslu čl. 64 odst. 1 a 2 zákona o ochraně osobních údajů odkazuje na porušení některé ze zásad, práv a povinností obsažených v zákoně na ochranu práv fyzických osob týkajících se osobních údajů". Totéž platí pro pravomoci Komise pro ochranu osobních údajů podle článku 45-4 zákona o používání a ochraně úvěrových informací.

([151]) Článek 60 prováděcí vyhlášky k zákonu o ochraně osobních údajů.

(123) Kromě svých nápravných pravomocí může Komise pro ochranu osobních údajů ukládat správní pokuty ve výši 10 až 50 milionů wonů za porušení různých požadavků zákona o ochraně osobních údajů (článek 75 zákona o ochraně osobních údajů) ([152]). To mimo jiné zahrnuje nedodržení požadavků na zákonnost zpracování, nepřijetí nezbytných bezpečnostních opatření, neinformování subjektů údajů v případě porušení zabezpečení údajů, nedodržení požadavků na dílčí zpracování, nestanovení a nezveřejnění zásad ochrany soukromí, nejmenování pověřence pro ochranu soukromí nebo nečinnost v případě žádosti subjektu údajů v rámci výkonu jeho individuálních práv a rovněž určitá procesní porušení (odepření spolupráce při vyšetřování). V případě porušení více ustanovení zákona o ochraně osobních údajů jedním správcem může být uložena pokuta za každé porušení, přičemž se při stanovení výše pokuty zohlední počet dotčených fyzických osob.

(124) Navíc, pokud existují přiměřené důvody pro podezření z porušení zákona o ochraně osobních údajů nebo jiných „právních předpisů o ochraně osobních údajů“, Komise pro ochranu osobních údajů může podat trestní oznámení u příslušného vyšetřovacího orgánu (např. státního zástupce, viz čl. 65 odst. 1 zákona o ochraně osobních údajů). Kromě toho může Komise pro ochranu osobních údajů správci doporučit, aby přijal disciplinární opatření vůči odpovědné osobě (včetně odpovědného vedoucího pracovníka, viz čl. 65 odst. 2 zákona o ochraně osobních údajů). Po obdržení takového doporučení je správce povinen je dodržet ([153]) a Komisi pro ochranu osobních údajů písemně oznámit výsledek (článek 65 zákona o ochraně osobních údajů ve spojení s článkem 58 prováděcí vyhlášky k zákonu o ochraně osobních údajů).

(125) Pokud jde o doporučení podle článku 61, nápravná opatření podle článku 64, obvinění nebo doporučení k disciplinárnímu řízení podle článku 65 a ukládání správních pokut podle článku 75 zákona o ochraně osobních údajů, Komise pro ochranu osobních údajů může zveřejnit skutkový stav (tj. dané porušení, subjekt, který porušil zákon, a uložená opatření), a to uvedením na svých internetových stránkách nebo v obecném celostátním deníku (článek 66 zákona o ochraně osobních údajů ve spojení s čl. 61 odst. 1 prováděcí vyhlášky k zákonu o ochraně osobních údajů) ([154]).

(126) A konečně dodržení požadavků na ochranu údajů podle zákona o ochraně osobních údajů (stejně jako jiných „právních předpisů o ochraně údajů“) podporuje i režim trestních sankcí. V tomto ohledu články 70 až 73 zákona o ochraně osobních údajů obsahují ustanovení o sankcích, která mohou vést k uložení pokuty (ve výši 20 až 100 milionů wonů) nebo k trestu odnětí svobody (s maximální sazbou od dvou do deseti let). Závažná porušení zahrnují mimo jiné použití osobních údajů nebo poskytnutí těchto údajů třetí straně bez potřebného souhlasu, zpracování citlivých informací v rozporu se zákazem podle čl. 23 odst. 1 zákona o ochraně osobních údajů, nedodržení platných bezpečnostních požadavků, které vede ke ztrátě, odcizení, vyzrazení, padělání, pozměnění nebo poškození osobních údajů, nepřijetí nezbytných opatření k opravě, výmazu nebo pozastavení zpracování osobních údajů nebo nezákonné předání osobních údajů do třetí země ([155]). Podle článku 74 zákona o ochraně osobních údajů nese v každém z těchto případů odpovědnost zaměstnanec, zástupce nebo představitel správce a rovněž samotný správce ([156]).

(127) Kromě trestních sankcí stanovených v zákoně o ochraně osobních údajů může zneužití osobních údajů představovat i trestný čin podle trestního zákona. Jedná se zejména o porušování listovního tajemství a narušení utajení dokumentů nebo elektronických záznamů (článek 316), vyzrazení informací podléhajících služebnímu tajemství (článek 317), podvody s využitím počítačů (článek 347-2) a také zpronevěru a porušení důvěry (článek 355).

(128) Korejský systém proto kombinuje různé druhy sankcí od nápravných opatření a správních pokut až po trestní sankce, které budou mít pravděpodobně zvláště silný odrazující účinek vůči správcům a osobám nakládajícím s údaji. Komise pro ochranu osobních údajů začala využívat svých pravomocí ihned po svém vzniku v roce 2020.

([152]) Pokud jsou navíc systémy zpracování a ochrany osobních údajů provozované správcem certifikovány jako systémy v souladu se zákonem o ochraně osobních údajů, avšak nebyla skutečně splněna certifikační kritéria podle čl. 34-2 odst. 1 prováděcí vyhlášky k zákonu o ochraně osobních údajů, nebo v případě závažného porušení jakéhokoli „právního předpisu o ochraně [osobních] údajů“, může Komise pro ochranu osobních údajů certifikaci zrušit (článek 32-2 odst. 3 a 5 zákona o ochraně osobních údajů). Komise pro ochranu osobních údajů vyrozumí správce o takovém zrušení certifikace a veřejně to oznámí nebo zveřejní na svých internetových stránkách nebo v úředním věstníku (článek 34-4 prováděcí vyhlášky k zákonu o ochraně osobních údajů). Za porušení zákona o používání a ochraně úvěrových informací jsou rovněž stanoveny správní pokuty (článek 52 zákona o používání a ochraně úvěrových informací) a trestní sankce (článek 50 zákona o používání a ochraně úvěrových informací).

([153]) Podle čl. 58 odst. 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů musí správce v případě, že kvůli zvláštním okolnostem je dodržení doporučení „neproveditelné“, poskytnout Komisi pro ochranu osobních údajů řádné odůvodnění.

([154]) Při rozhodování, zda takové zveřejnění provede, zohlední Komise pro ochranu osobních údajů podstatu a závažnost porušení, jeho délku trvání a četnost a také jeho následky (rozsah škody). Dotčený subjekt bude předem vyrozuměn a bude mu poskytnuta možnost obhajoby. Viz čl. 61 odst. 2 a 3 prováděcí vyhlášky k zákonu o ochraně osobních údajů.

([155]) Viz čl. 71 bod 2 ve spojení s čl. 18 odst. 1 zákona o ochraně osobních údajů (nedodržení podmínek čl. 17 odst. 3 zákona o ochraně osobních údajů, na který odkazuje čl. 18 odst. 1). Viz také čl. 75 odst. 2 bod 1 ve spojení s čl. 17 odst. 2 zákona o ochraně osobních údajů (neposkytnutí nezbytných informací dotčené fyzické osobě podle čl. 17 odst. 2 zákona o ochraně osobních údajů, na který odkazuje čl. 17 odst. 3).

([156]) Kromě toho článek 74-2 zákona o ochraně osobních údajů umožňuje zabavení jakýchkoli peněžních prostředků, zboží nebo jiných zisků získaných v důsledku porušení, nebo v případě, že není zabavení možné, „výběr“ nezákonně získaného prospěchu.

Výroční zpráva Komise pro ochranu osobních údajů za rok 2021 ukazuje, že Komise pro ochranu osobních údajů již vydala řadu doporučení, správních pokut a nápravných příkazů, které se týkaly jak veřejného sektoru (34 veřejných orgánů), tak soukromých subjektů (přibližně 140 společností) ([157]). Mezi významné případy patří například uložení pokuty jedné společnosti ve výši 6,7 miliardy wonů v prosinci 2020 za porušení různých ustanovení zákona o ochraně osobních údajů (včetně bezpečnostních požadavků, požadavků na souhlas s poskytováním třetí straně a transparentnost) ([158]) a uložení pokuty v dubnu 2021 ve výši 103,3 milionu wonů společnosti zabývající se technologií umělé inteligence, mimo jiné za porušení pravidel zákonnosti zpracování, zejména souhlasu, a zpracování pseudonymizovaných údajů ([159]). V srpnu 2021 dokončila Komise pro ochranu osobních údajů další vyšetřování činnosti tří společností, jež vyústila v nápravná opatření a uložení pokut ve výši až 6,47 miliardy wonů (mimo jiné za neinformování fyzických osob o zpřístupnění jejich osobních údajů třetím stranám, včetně předání údajů do třetích zemí) ([160]). Již před nedávnou reformou měla Jižní Korea dobré výsledky v oblasti vymáhání práva, přičemž odpovědné orgány využívaly celou škálu donucovacích opatření, včetně správních pokut, nápravných opatření a „uvedení jména a sdílení“, vůči různým správcům, včetně poskytovatelů komunikačních služeb (Korejská komise pro komunikace), a také komerčním hospodářským subjektům, finančním institucím, veřejným orgánům, univerzitám a nemocnicím (Ministerstvo vnitra a bezpečnosti) ([161]). Na tomto základě dospěla komise k závěru, že korejský systém zajišťuje účinné prosazování pravidel ochrany údajů v praxi, a tím zaručuje úroveň ochrany v zásadě rovnocennou úrovni podle nařízení (EU) 2016/679.

2.5 **Opravné prostředky**

(129) Aby se zajistila odpovídající ochrana a zejména vymáhání individuálních práv, měla by být subjektu údajů poskytnuta účinná správní a soudní ochrana, včetně náhrady škody.

(130) Korejský systém poskytuje fyzickým osobám různé mechanismy k účinnému vymáhání jejich práv a získání (soudní) ochrany.

(131) Jako první krok se mohou fyzické osoby, které mají za to, že jejich práva nebo zájmy na ochranu údajů byly porušeny, obrátit na příslušného správce. Podle čl. 30 odst. 1 bodu 5 zákona o ochraně osobních údajů musí zásady ochrany osobních údajů správce mimo jiné obsahovat informace o právech subjektů údajů a o způsobech jejich výkonu. Kromě toho musí uvádět kontaktní informace (např. jméno a telefonní číslo pověřence pro ochranu soukromí nebo oddělení odpovědného za ochranu údajů), aby bylo možné podávat stížnosti. V rámci organizace správce existuje pověřenec pro ochranu osobních údajů, který se zabývá vyřizováním stížností, přijímáním nápravných opatření v případě porušení soukromí a řešením odškodnění (čl. 31 odst. 2 bod 3 a odst. 4 zákona o ochraně osobních údajů). Posledně uvedené je důležité například v případě porušení zabezpečení údajů, neboť správce musí mimo jiné subjektu údajů sdělit kontaktní místo (místa) pro nahlášení jakékoli škody (čl. 34 odst. 1 bod 5 zákona o ochraně osobních údajů).

(132) Zákon o ochraně osobních údajů navíc nabízí několik možností opravných prostředků fyzických osob vůči správcům. Zaprvé může každá fyzická osoba, jež má za to, že správce porušil její práva nebo zájmy v oblasti ochrany údajů, toto porušení nahlásit přímo Komisi pro ochranu osobních údajů a/nebo jedné ze specializovaných institucí jmenovaných Komisí pro ochranu osobních údajů k přijímání a vyřizování stížností; to zahrnuje Korejskou agenturu pro internet a bezpečnost, která za tímto účelem provozuje kontaktní centrum pro ochranu osobních údajů (tzv. „kontaktní centrum pro ochranu soukromí“) (čl. 62 odst. 1 a 2 zákona o ochraně osobních údajů ve spojení s článkem 59 prováděcí vyhlášky k zákonu o ochraně osobních údajů). Kontaktní centrum pro ochranu soukromí vyšetřuje a zjišťuje případy porušení předpisů, poskytuje poradenství v souvislosti se zpracováním osobních údajů (čl. 62 odst. 3 zákona o ochraně osobních údajů) a může porušení oznámit Komisi pro

([157]) Viz výroční zpráva Komise pro ochranu osobních údajů za rok 2021, s. 50–55 (dostupná pouze v korejštině) na adrese https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK

([158]) Viz (dostupné pouze v korejštině) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) Viz (dostupné pouze v korejštině) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4l7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) Viz (dostupné pouze v korejštině) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Viz např. výroční zpráva za rok 2020 (dostupná pouze v korejštině) na adrese https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 a příklady v anglickém jazyce na adrese https://www.privacy.go.kr/eng/enforcement_02.do.

ochranu osobních údajů (ale samo nemůže přijmout donucovací opatření). Kontaktní centrum pro ochranu soukromí dostává velké množství stížností/žádostí (např. 177 457 v roce 2020, 159 255 v roce 2019 a 164 497 v roce 2018) ([162]). Podle informací získaných od Komise pro ochranu osobních údajů obdržela jen tato komise v období od srpna 2020 do srpna 2021 asi 1 000 stížností. V reakci na stížnost může Komise pro ochranu osobních údajů vydat doporučení ke zlepšení, podniknout nápravná opatření, vydat „obvinění" u příslušného vyšetřovacího orgánu (včetně státního zástupce) nebo doporučit disciplinární opatření (viz články 61, 64 a 65 zákona o ochraně osobních údajů). Rozhodnutí Komise pro ochranu osobních údajů (např. odmítnutí zabývat se stížností nebo zamítnutí stížnosti z věcných důvodů) lze napadnout podle zákona o správním řízení ([163]).

(133) Zadruhé podle článků 40 až 50 zákona o ochraně osobních údajů ve spojení s články 48-14 až 57 prováděcí vyhlášky k zákonu o ochraně osobních údajů mohou subjekty údajů vznášet nároky u tzv. „mediačního výboru", který se skládá ze zástupců jmenovaných předsedou Komise pro ochranu osobních údajů z řad členů vyšších výkonných pracovníků komise a jednotlivců jmenovaných na základě jejich praxe v oblasti ochrany údajů z určitých způsobilých skupin (viz čl. 40 odst. 2, 3 a 7 zákona o ochraně osobních údajů, článek 48-14 prováděcí vyhlášky k zákonu o ochraně osobních údajů) ([164]). Možnost využít mediace u mediačního výboru poskytuje alternativní cestu, jak dosáhnout nápravy, ale neomezuje právo fyzické osoby obrátit se místo toho na Komisi pro ochranu osobních údajů nebo na soudy. Za účelem prošetření případu může výbor požádat strany sporu, aby poskytly potřebné materiály, a/nebo vyzvat příslušné svědky, aby se k výboru dostavili (článek 45 zákona o ochraně osobních údajů). Po vyjasnění věci výbor vypracuje návrh mediačního nálezu ([165]), na kterém se musí shodnout většina jeho členů. Návrh mediačního nálezu může zahrnovat zastavení porušení, nezbytná nápravná opatření (včetně navrácení do původního stavu nebo odškodnění) a rovněž jakákoli opatření nezbytná k zabránění opakování téhož nebo podobného porušení (čl. 47 odst. 1 zákona o ochraně osobních údajů). Pokud obě strany s mediačním nálezem souhlasí, bude mít stejný účinek jako soudní smír (čl. 47 odst. 5 zákona o ochraně osobních údajů). Žádné ze stran není během mediace bráněno v podání návrhu na zahájení soudního řízení a v takovém případě bude mediace pozastavena (viz čl. 48 odst. 2 zákona o ochraně osobních údajů) ([166]). Roční údaje Komise pro ochranu osobních údajů ukazují, že fyzické osoby pravidelně využívají řízení u mediačního výboru, jež často vede k úspěšnému výsledku. Například v roce 2020 se výbor zabýval 126 případy, z nichž 89 bylo vyřešeno před výborem (v 77 případech strany dosáhly dohody již před skončením mediačního řízení a ve 12 případech strany mediační návrh přijaly), takže míra mediace činila 70,6 % ([167]). Podobně se výbor v roce 2019 zabýval 139 případy, z nichž 92 bylo vyřešeno, takže míra mediace činila 62,2 %.

(134) Pokud navíc újmu utrpí alespoň 50 fyzických osob nebo jsou porušena jejich práva na ochranu údajů stejným nebo podobným způsobem v důsledku stejného (druhu) incidentu ([168]), může subjekt údajů nebo organizace na ochranu údajů podat návrh na kolektivní mediaci sporu jménem takové skupiny; další subjekty údajů mohou požádat o připojení se k takové mediaci, kterou mediační výbor veřejně oznámí (čl. 49 odst. 1 až 3 zákona o ochraně osobních údajů ve spojení s články 52 až 54 prováděcí vyhlášky k zákonu o ochraně osobních údajů) ([169]). Mediační výbor může jako zastupující stranu vybrat alespoň jednu osobu, která nejlépe zastupuje

([162]) Viz výroční zpráva Komise pro ochranu osobních údajů za rok 2021, s. 174. Tyto stížnosti se v roce 2020 týkaly mimo jiné shromažďování údajů bez souhlasu subjektu údajů, nedodržení povinností týkajících se transparentnosti, porušení zákona o ochraně osobních údajů zpracovateli, nedostatečných bezpečnostních opatření, nereagování na žádosti subjektů údajů, jakož i obecných šetření.

([163]) Konkrétně mohou fyzické osoby podat opravný prostředek proti výkonu veřejné moci nebo proti odmítnutí provést výkon veřejné moci ze strany správního úřadu (čl. 2 odst. 1 bod 1, čl. 3 bod 1 zákona o správním soudním řízení). Podrobnější informace o procesních aspektech, včetně požadavků na přípustnost, uvádí 181. bod odůvodnění.

([164]) Všichni členové mají pevně stanovené funkční období a mohou být odvoláni pouze z oprávněného důvodu (viz čl. 40 odst. 5 a článek 41 zákona o ochraně osobních údajů). Kromě toho článek 42 zákona o ochraně osobních údajů obsahuje záruky na ochranu před střety zájmů.

([165]) Viz článek 44 zákona o ochraně osobních údajů. Kromě toho může výbor navrhnout návrh narovnání a doporučit narovnání bez mediace (viz článek 46 zákona o ochraně osobních údajů).

([166]) Výbor také může mediaci odmítnout, má-li za to, že mediace sporu není vhodná s ohledem na jeho povahu nebo vzhledem k tomu, že návrh na mediaci byl podán za nekalým účelem (článek 48 zákona o ochraně osobních údajů).

([167]) Viz výroční zpráva Komise pro ochranu osobních údajů za rok 2021, s. 179–180. Tyto případy se týkaly mimo jiné porušení povinnosti získat souhlas se shromažďováním údajů, zásady účelového omezení a práv subjektu údajů.

([168]) Viz čl. 49 odst. 1 zákona o ochraně osobních údajů, podle kterého musí subjekty údajů utrpět škodu nebo jejich práva musí být porušena „stejným nebo podobným způsobem", a čl. 52 bod 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů, který požaduje, aby „[z]ásadní prvky incidentu byly věcně nebo právně společné".

([169]) Z mediačního nálezu v kolektivním sporu akceptovaného správcem mohou mít prospěch i nezúčastněné strany, neboť mediační výbor může správci doporučit, aby vypracoval a předložil plán odškodnění, který zahrnuje (také) tyto strany (čl. 49 odst. 5 zákona o ochraně osobních údajů).

společný zájem (čl. 49 odst. 4 zákona o ochraně osobních údajů). Pokud správce odmítne mediaci kolektivního sporu nebo neakceptuje mediační nález, mohou některé organizace ([170]) podat hromadnou žalobu ve věci porušení práv (články 51 až 57 zákona o ochraně osobních údajů).

(135) Zatřetí, v případě porušení soukromí způsobujícího „škodu" fyzické osobě má subjekt údajů právo na přiměřenou nápravu v „rychlém a spravedlivém řízení" (čl. 4 bod 5 a článek 39 zákona o ochraně osobních údajů) ([171]). Správce se může vyvinit tím, že prokáže neexistenci zavinění („nezákonného úmyslu" nebo nedbalosti). Utrpí-li subjekt údajů škodu v důsledku ztráty, odcizení, vyzrazení, padělání, pozměnění nebo poškození jeho osobních údajů, může soud stanovit odškodnění až do výše trojnásobku skutečné škody, přičemž zohlední řadu faktorů (čl. 39 odst. 3 a 4 zákona o ochraně osobních údajů). Alternativně může subjekt údajů požadovat „přiměřenou částku" odškodnění nepřesahující 3 miliony wonů (článek 39-2 odst. 1 a 2 zákona o ochraně osobních údajů). Náhradu škody lze navíc v souladu s občanským zákoníkem požadovat od každé osoby, „která jiné osobě protiprávním jednáním úmyslně nebo z nedbalosti způsobí škodu nebo újmu na zdraví" ([172]), nebo od osoby, „která způsobila osobní újmu, újmu na svobodě nebo pověsti jiné osoby nebo jiné osobě způsobila duševní útrapy" ([173]). Takovou odpovědnost za delikt vyplývající z porušení pravidel ochrany údajů potvrdil Nejvyšší soud ([174]). Byla-li škoda způsobena nezákonným postupem orgánu veřejné správy, lze dále uplatnit nárok na odškodnění podle zákona o náhradě škody státem ([175]). Žalobu podle zákona o náhradě škody státem lze podat u specializované „rady pro náhradu škody" nebo přímo u korejských soudů ([176]). Odpovědnost státu se vztahuje i na nemateriální újmu (např. duševní utrpení) ([177]). Je-li obětí cizí státní příslušník, použije se zákon o náhradě škody státem, pokud příslušná země původu zajišťuje rovnocenným způsobem náhradu škody státem pro korejské státní příslušníky ([178]).

(136) Začtvrté Nejvyšší soud uznal, že fyzické osoby mají právo domáhat se soudního zákazu při porušení jejich práv podle ústavy, včetně práva na ochranu osobních údajů ([179]). V této souvislosti může soud například nařídit správcům, aby pozastavili nebo ukončili jakoukoli nezákonnou činnost. Práva na ochranu údajů včetně práv chráněných zákona o ochraně osobních údajů lze navíc vymáhat občanskoprávními žalobami. Tuto horizontální aplikaci ústavní ochrany soukromí na vztahy mezi soukromými osobami uznal i Nejvyšší soud ([180]).

([170]) Jmenovitě spotřebitelské skupiny nebo neziskové nevládní organizace určité velikosti z hlediska počtu členů, jejichž účelem činnosti je ochrana údajů (přestože v případě posledně jmenovaných platí dodatečný požadavek, aby hromadnou žalobu podalo alespoň 100 subjektů údajů, které byly předmětem stejného (druhu) porušení. Viz článek 51 zákona o ochraně osobních údajů.

([171]) Články 43 až 43-3 zákona o používání a ochraně úvěrových informací stanoví rovněž odpovědnost za náhradu škody vyplývající z porušení tohoto zákona.

([172]) Článek 750 občanského zákoníku.

([173]) Ustanovení čl. 751 odst. 1 občanského zákoníku.

([174]) Viz například rozhodnutí Nejvyššího soudu 2015Da251539, 251546, 251553, 251560, 251577, 30. května 2018. Kromě toho Nejvyšší soud potvrdil, že porušení zabezpečení údajů mohou vést k přiznání náhrady škody podle občanského zákoníku, viz rozhodnutí Nejvyššího soudu 2011Da59834, 59858, 59841, 26. prosince 2012 (shrnutí v anglickém jazyce je k dispozici na adrese http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). V této věci Nejvyšší soud objasnil, že pro posouzení toho, zda fyzická osoba utrpěla emocionální újmu kvalifikovanou jako nahraditelná škoda, je třeba vzít v úvahu několik faktorů, jako je druh a charakteristika uniklých údajů, identifikovatelnost fyzické osoby v důsledku narušení zabezpečení údajů, možnost přístupu třetích stran k údajům, rozsah, v němž byly osobní údaje šířeny, zda to vedlo k dalšímu porušování individuálních práv, jak byly osobní údaje spravovány a chráněny atd.

([175]) Podle zákona o náhradě škody státem mohou fyzické osoby žádat o náhradu škody způsobené státními úředníky při výkonu jejich služebních povinností v rozporu se zákonem (čl. 2 odst. 1 zákona).

([176]) Články 9 a 12 zákona o náhradě škody státem. Zákon zřizuje okresní rady (kterým předsedá náměstek státního zástupce příslušného státního zastupitelství), ústřední radu (které předsedá náměstek ministra spravedlnosti) a zvláštní radu (která vyřizuje nároky na náhradu škody způsobené vojenským personálem nebo civilními zaměstnanci armády a předsedá jí náměstek ministra národní obrany). Žádosti o náhradu škody zpravidla vyřizují okresní rady, které musí za určitých okolností postoupit věc ústřední/zvláštní radě, např. pokud náhrada škody přesáhne určitou částku nebo pokud jednotlivec požádá o opětovné projednání. Všechny rady se skládají z členů jmenovaných ministrem spravedlnosti (např. z řad úředníků Ministerstva spravedlnosti, soudních znalců, advokátů a osob se zkušenostmi v oblasti náhrad škody státem) a podléhají zvláštním pravidlům pro střet zájmů (viz článek 7 prováděcí vyhlášky k zákonu o náhradě škody státem).

([177]) Viz článek 8 zákona o náhradě škody státem (který odkazuje na občanský zákoník) a rovněž článek 751 občanského zákoníku.

([178]) Článek 7 zákona o náhradě škody státem.

([179]) Rozhodnutí Nejvyššího soudu 93Da40614, 12. dubna 1996, a rozhodnutí 2008Da42430, 2. září 2011 (shrnutí v anglickém jazyce je k dispozici na adrese https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Viz například rozhodnutí Nejvyššího soudu 2008Da42430, 2. září 2011 (shrnutí v anglickém jazyce je k dispozici na adrese https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) A konečně mohou fyzické osoby podat trestní oznámení podle zákona o trestním řízení (článku 223) státnímu zástupci nebo příslušníkovi soudní policie ([181]).

(138) Korejský systém tedy nabízí různé druhy opravných prostředků od snadno dostupných nízkonákladových možností (například kontaktováním kontaktního centra pro ochranu soukromí nebo prostřednictvím (kolektivní) mediace) až po prostředky správní (u Komise pro ochranu osobních údajů) a soudní, včetně možnosti získat náhradu škody.

3. PŘÍSTUP K OSOBNÍM ÚDAJŮM PŘEDÁVANÝM Z EVROPSKÉ UNIE A JEJICH POUŽITÍ ORGÁNY VEŘEJNÉ MOCI V KOREJSKÉ REPUBLICE

(139) Komise také posuzovala omezení a záruky, včetně dozoru a jednotlivých ochranných mechanismů dostupných v korejském právu, pokud jde o shromažďování a následné používání osobních údajů předávaných správcům v Koreji ze strany korejských orgánů veřejné správy pro účely veřejného zájmu, zejména pro účely prosazování trestního práva a národní bezpečnosti (dále jen „přístup vlády“). V tomto ohledu korejská vláda předložila Komisi oficiální prohlášení, ujištění a závazky podepsané na nejvyšší úrovni ministerstev a orgánů, které jsou obsaženy v příloze II tohoto rozhodnutí.

(140) Při posuzování toho, zda podmínky přístupu vlády k údajům předávaným do Koreje podle tohoto rozhodnutí splňují test „zásadní rovnocennosti“ podle čl. 45 odst. 1 nařízení (EU) 2016/679, jak je vykládán Soudním dvorem Evropské unie ve světle Listiny základních práv, Komise zohlednila zejména následující kritéria.

(141) Zaprvé musí být jakékoli omezení práva na ochranu osobních údajů stanoveno zákonem a samotný právní základ, který umožňuje zásah do takového práva, musí vymezovat rozsah omezení výkonu dotčeného práva ([182]).

(142) Zadruhé, za účelem splnění požadavku proporcionality, podle kterého musí být výjimky z ochrany osobních údajů a její omezení činěny v mezích toho, co je v demokratické společnosti nezbytně nutné pro splnění konkrétních cílů obecného zájmu rovnocenných cílům uznaným Unií, musí předmětná právní úprava třetí země, která daný zásah povoluje, stanovit jasná a přesná pravidla pro rozsah a použití předmětného opatření a stanovit minimální požadavky, tak aby osoby, jejichž údaje byly předány, měly dostatečné záruky umožňující účinně chránit své osobní údaje proti riziku zneužití ([183]). Právní úprava musí zejména vymezit okolnosti a podmínky, za nichž může být přijato opatření týkající se zpracování takových údajů ([184]), jakož i podřizovat plnění takových požadavků nezávislému dozoru ([185]).

(143) Zatřetí musí být tato právní úprava podle vnitrostátního práva právně závazná. Týká se to především orgánů dotčené třetí země, tyto právní požadavky však musí být vůči těmto orgánům rovněž vymahatelné u soudu ([186]). Subjekty údajů musí mít zejména možnost podat žalobu k nezávislému a nestrannému soudu pro získání přístupu ke svým osobním údajům nebo pro dosažení opravy nebo výmazu takovýchto údajů ([187]).

3.1 **Obecný právní rámec**

(144) Omezení a záruky týkající se shromažďování a následného používání osobních údajů korejskými orgány veřejné správy vyplývají ze zastřešujícího ústavního rámce, zvláštních právních předpisů, které upravují jejich činnost v oblasti vymáhání trestního práva a národní bezpečnosti, jakož i z pravidel, která se konkrétně vztahují na zpracování osobních údajů.

([181]) Jak vysvětluje 127. bod odůvodnění, zneužití údajů může představovat trestný čin podle trestního zákona.
([182]) Viz rozsudek ve věci Schrems II, body 174–175 a citovaná judikatura. Pokud jde o přístup orgánů veřejné správy členských států, viz také věc C-623/17 Privacy International, ECLI:EU:C:2020:790, bod 65 a spojené věci C-511/18, C-512/18 a C-520/18 La Quadrature du Net a další, ECLI:EU:C:2020:791, bod 175.
([183]) Viz rozsudek ve věci Schrems II, body 176 a 181, jakož i citovaná judikatura. Pokud jde o přístup orgánů veřejné správy členských států, viz také věc Privacy International, bod 68; a La Quadrature du Net a další, bod 132.
([184]) Viz rozsudek ve věci Schrems II, bod 176. Pokud jde o přístup orgánů veřejné správy členských států, viz také věc Privacy International, bod 68; a La Quadrature du Net a další, bod 132.
([185]) Viz rozsudek ve věci Schrems II, bod 179.
([186]) Viz rozsudek ve věci Schrems II, body 181–182.
([187]) Viz rozsudek ve věci Schrems, bod 95 a rozsudek ve věci Schrems II, bod 194. V tomto ohledu SDEU zejména zdůraznil, že dodržování článku 47 Listiny základních práv Evropské unie, který zaručuje právo na účinnou ochranu nezávislým a nestranným soudem nebo tribunálem, „spolutvoří úroveň ochrany vyžadovanou v Unii a [jeho] dodržení musí Komise konstatovat ještě před přijetím rozhodnutí o odpovídající ochraně na základě čl. 45 odst. 1 [nařízení (EU) 2016/679]“ (rozsudek ve věci Schrems II, bod 186).

(145) Zaprvé se přístup korejských orgánů veřejné správy k osobním údajům řídí obecnými zásadami zákonnosti, nezbytnosti a proporcionality, které vyplývají z korejské ústavy ([188]). Konkrétně základní práva a svobody (včetně práva na soukromí a práva na důvěrnost korespondence) ([189]) mohou být omezeny pouze zákonem, a pouze pokud je to nezbytné pro národní bezpečnost nebo pro zachování práva a pořádku v zájmu veřejného blaha. Taková omezení se nesmí dotknout podstaty dotčeného práva nebo svobody. Pokud jde konkrétně o prohlídky a zajištění věcí, ústava stanoví, že se mohou uskutečnit pouze tak, jak stanoví zákon, na základě příkazu vydaného soudcem a při dodržení řádného postupu ([190]). A konečně se fyzické osoby mohou dovolávat svých práv a svobod u Ústavního soudu, mají-li za to, že tato práva a svobody poškodily orgány veřejné správy při výkonu své pravomoci ([191]). Stejně tak fyzické osoby, které utrpěly škodu v důsledku protiprávního jednání státního úředníka při plnění jeho úředních povinností, mají právo požadovat spravedlivé odškodnění ([192]).

(146) Zadruhé, jak je podrobněji popsáno v oddílech 3.2.1 a 3.3.1, obecné zásady uvedené ve 145. bodě odůvodnění se odrážejí také ve zvláštních právních předpisech, které upravují pravomoci donucovacích orgánů a vnitrostátních bezpečnostních orgánů. Například pokud jde o vyšetřování trestné činnosti, zákon o trestním řízení stanoví, že povinná opatření mohou být přijata pouze tehdy, je-li to výslovně stanoveno v zákoně o trestním řízení, a to v nejmenším rozsahu nezbytném k dosažení účelu vyšetřování ([193]). Podobně článek 3 zákona o ochraně soukromí v komunikacích zakazuje přístup k soukromé komunikaci s výjimkou přístupu na základě právních předpisů a s výhradou omezení a záruk v nich stanovených. V oblasti národní bezpečnosti zákon o Národní zpravodajské službě stanoví, že jakýkoli přístup ke komunikaci nebo informacím o poloze musí být v souladu se zákonem a na zneužití pravomoci a porušení zákona se vztahují trestní sankce ([194]).

(147) Zatřetí zpracování osobních údajů orgány veřejné správy, a to i pro účely prosazování práva a národní bezpečnosti, podléhá pravidlům ochrany údajů podle zákona o ochraně osobních údajů ([195]). Obecně čl. 5 odst. 1 zákona o ochraně osobních údajů vyžaduje, aby orgány veřejné správy vypracovaly zásady, které mají zabránit „zneužívání a neoprávněnému užívání osobních údajů, indiskrétnímu dohledu a sledování atd. a posílit důstojnost lidských bytostí a soukromí jednotlivců“. Kromě toho musí každý správce zpracovávat osobní údaje způsobem, který minimalizuje možnost narušení soukromí subjektu údajů (čl. 3 odst. 6 zákona o ochraně osobních údajů).

(148) Všechny požadavky zákona o ochraně osobních údajů, podrobně popsané v oddíle 2, se vztahují na zpracování osobních údajů pro účely prosazování práva. Zahrnuje to základní zásady (jako je zákonnost a korektnost, účelové omezení, přesnost, minimalizace údajů, omezení uložení, zabezpečení a transparentnost), povinnosti (například pokud jde o oznámení porušení zabezpečení údajů a citlivé údaje) a práva (na přístup, opravu, výmaz a pozastavení zpracování).

(149) Zatímco zpracování osobních údajů pro účely národní bezpečnosti podléhá omezenějšímu souboru ustanovení podle zákona o ochraně osobních údajů, platí základní zásady, jakož i pravidla pro dozor, vymáhání a ochranu ([196]). Přesněji řečeno, články 3 a 4 zákona o ochraně osobních údajů stanoví obecné zásady ochrany údajů (zákonnost a korektnost, účelové omezení, přesnost, minimalizace údajů, zabezpečení a transparentnost) a individuální práva (právo být informován, právo na přístup a práva na opravu, výmaz a pozastavení zpracování) ([197]). Ustanovení čl. 4 odst. 5 zákona o ochraně osobních údajů dále dává fyzickým osobám právo na přiměřenou náhradu jakékoli škody vzniklé v důsledku zpracování takových osobních údajů, a to prostřednictvím

([188]) Viz příloha II oddíl 1.1.
([189]) Ustanovení čl. 37 odst. 2 ústavy.
([190]) Článek 16 a čl. 12 odst. 3 ústavy. Ustanovení čl. 12 odst. 3 ústavy dále vyjmenovává výjimečné okolnosti, za nichž může dojít k prohlídkám nebo zajištění věcí bez soudního příkazu (jakkoli je stále vyžadován soudní příkaz vydaný následně), tj. za situace *in flagrante delicto* nebo u trestných činů podléhajících trestu odnětí svobody v délce nejméně tří let, pokud existuje riziko, že budou zničeny důkazy nebo podezřelý uprchne.
([191]) Ustanovení čl. 68 odst. 1 zákona o Ústavním soudu.
([192]) Ustanovení čl. 29 odst. 1 ústavy.
([193]) Ustanovení čl. 199 odst. 1 zákona o trestním řízení. Obecněji řečeno, při výkonu svých pravomocí podle zákona o trestním řízení musí orgány veřejné správy respektovat základní práva podezřelých z trestné činnosti a všech dalších dotčených osob (čl. 198 odst. 2 zákona o trestním řízení).
([194]) Článek 14 zákona o Národní zpravodajské službě.
([195]) Viz příloha II oddíl 1.2.
([196]) Ustanovení čl. 58 odst. 1 bodu 2 zákona o ochraně osobních údajů. Viz také oddíl 6 oznámení č. 2021-5 (příloha I). Tato výjimka z určitých ustanovení zákona o ochraně osobních údajů se vztahuje pouze na zpracování osobních údajů „pro účely národní bezpečnosti“. Po skončení události v oblasti národní bezpečnosti, která zpracování údajů odůvodňuje, se již této výjimky nelze dovolávat a použijí se všechny povinnosti podle zákona o ochraně osobních údajů.
([197]) Taková práva mohou být omezena pouze tehdy, stanoví-li to zákon, a to v rozsahu a po dobu, kdy je to nezbytné a přiměřené k ochraně důležitého cíle veřejného zájmu, nebo pokud by poskytnutí práva mohlo způsobit újmu na životě nebo zdraví třetí osoby nebo neoprávněný zásah do majetkových a jiných zájmů třetí strany. Viz oddíl 6 oznámení č. 2021-5.

rychlého a spravedlivého řízení. To doplňují specifičtější povinnosti zpracovávat osobní údaje pouze v minimálním rozsahu nezbytném k dosažení zamýšleného účelu a po minimální dobu, zavést nezbytná opatření k zajištění bezpečné správy údajů a vhodného zpracování (jako jsou technické, řídicí a fyzické záruky), jakož i zavést opatření pro vhodné vyřizování jednotlivých stížností ([198]). A konečně se na zpracování osobních údajů pro účely národní bezpečnosti vztahují i obecné zásady zákonnosti, nezbytnosti a proporcionality podle korejské ústavy (viz 145. bod odůvodnění).

(150) Těchto obecných omezení a záruk se mohou fyzické osoby pro dosažení ochrany dovolávat u nezávislých dozorových subjektů (např. Komise pro ochranu osobních údajů a/nebo Národní komise pro lidská práva, viz 177. a 178. bod odůvodnění) a soudů (viz 179. až 183. bod odůvodnění).

3.2 **Přístup korejských orgánů veřejné správy k osobním údajům a jejich použití těmito orgány pro účely prosazování trestního práva**

(151) Právo Korejské republiky ukládá řadu omezení přístupu k osobním údajům a použití těchto údajů pro účely prosazování trestního práva a stanoví dozorové a ochranné mechanismy, které jsou v souladu s požadavky uvedenými ve 141. až 143. bodě odůvodnění tohoto rozhodnutí. Podmínky, za kterých lze takový přístup uskutečnit, a záruky týkající se využívání těchto pravomocí jsou podrobně posouzeny v následujících oddílech.

3.2.1 *Právní základy, omezení a záruky*

(152) Korejské orgány mohou shromažďovat osobní údaje zpracovávané korejskými správci, které byly předány z Unie podle tohoto rozhodnutí ([199]), pro účely vymáhání trestního práva v souvislosti s prohlídkou nebo zajištěním věci (na základě zákona o trestním řízení), prostřednictvím přístupu k informacím o komunikaci (na základě zákona o ochraně důvěrnosti komunikací) nebo získáváním údajů účastníků prostřednictvím žádostí o dobrovolné zpřístupnění (na základě zákona o telekomunikačních službách) ([200]).

3.2.1.1 Prohlídky a zajištění věci

(153) Zákon o trestním řízení stanoví, že k prohlídce nebo zajištění věci může dojít pouze v případě, že je osoba podezřelá z trestného činu, je to nezbytné pro vyšetřování a je prokázáno spojení mezi vyšetřováním a osobou, která má být prohledána, nebo věcí, která má být zkontrolována nebo zajištěna ([201]). Kromě toho lze prohlídku nebo zajištění věci (jako každé povinné opatření) povolit pouze v nejmenším nezbytném rozsahu ([202]). Pokud je předmětem prohlídky počítačový disk nebo jiné médium pro ukládání dat, budou v zásadě zajištěna pouze nezbytná samotná data (zkopírovaná nebo vytištěná), nikoli celé médium ([203]). Médium lze zajistit pouze za předpokladu, že je považováno za v podstatě nemožné vytisknout nebo zkopírovat požadovaná data samostatně, nebo pokud je považováno za v podstatě neproveditelné naplnit účel prohlídky jinak ([204]). Zákon o trestním řízení proto stanoví jasná a přesná pravidla pro oblasti působnosti a použití těchto opatření, čímž zajišťuje, že zásah do práv jednotlivců v případě prohlídky nebo zajištění věci bude omezen na to, co je nezbytné pro konkrétní vyšetřování trestného činu a přiměřené sledovanému účelu.

([198]) Ustanovení čl. 58 odst. 4 zákona o ochraně osobních údajů.

([199]) Viz příloha II oddíl 2.1. Oficiální prohlášení korejské vlády (oddíl 2.1 přílohy II) také uvádí možnost shromažďovat informace o finančních transakcích za účelem předcházení praní špinavých peněz a financování terorismu na základě zákona o oznamování a používání určitých informací o finančních transakcích. Zákon o oznamování a používání určitých informací o finančních transakcích však ukládá povinnost zveřejňování pouze správcům, kteří zpracovávají osobní úvěrové informace podle zákona o používání a ochraně úvěrových informací a podléhají dozoru Komise pro finanční služby (viz 13. bod odůvodnění). Vzhledem k tomu, že zpracování osobních úvěrových informací takovými správci je vyloučeno z oblasti působnosti tohoto rozhodnutí, není zákon o oznamování a používání určitých informací o finančních transakcích pro toto posouzení relevantní.

([200]) Článek 3 zákona o ochraně důvěrnosti komunikací také zmiňuje zákon o vojenském soudu jako možný právní základ shromažďování komunikačních údajů. Tento zákon však upravuje shromažďování údajů o příslušnících armády a na civilní osoby je použitelný pouze v omezeném počtu případů (např. pokud by příslušníci armády a civilní osoby spáchali trestný čin společně nebo pokud by se fyzická osoba dopustila trestného činu proti armádě, může být zahájeno řízení před vojenským soudem, viz článek 2 zákona o vojenském soudu). V každém případě stanoví obecná ustanovení upravující prohlídky a zajištění věci, která jsou podobná zákonu o trestním řízení (viz např. články 146 až 149 a 153 až 156 zákona o vojenském soudu), a například stanoví, že poštovní zásilky mohou být shromažďovány pouze tehdy, je-li to nezbytné pro vyšetřování, a pouze na základě příkazu vojenského soudu. Bude-li shromažďována elektronická komunikace na základě tohoto zákona, použijí se omezení a záruky podle zákona o ochraně důvěrnosti komunikací. Viz příloha II oddíl 2.2.2 a poznámka pod čarou č. 50.

([201]) Ustanovení čl. 215 odst. 1 a 2 zákona o trestním řízení. Viz také čl. 106 odst. 1, články 107 a 109 zákona o trestním řízení, které stanoví, že soudy mohou provádět prohlídky a zajištění věci, pokud mají za to, že dotčené předměty nebo osoby souvisejí s konkrétní trestní věcí. Viz příloha II oddíl 2.2.1.2.

([202]) Ustanovení čl. 199 odst. 1 zákona o trestním řízení.

([203]) Ustanovení čl. 106 odst. 3 zákona o trestním řízení.

([204]) Ustanovení čl. 106 odst. 3 zákona o trestním řízení.

(154) Pokud jde o procesní záruky, zákon o trestním řízení vyžaduje, aby byl od soudu získán soudní příkaz k provedení prohlídky nebo zajištění věci ([205]). Prohlídka nebo zajištění věci bez soudního příkazu jsou přípustné jen výjimečně, a to v naléhavých případech ([206]), *in loco* v okamžiku zatčení nebo zadržení osoby podezřelé z trestného činu ([207]) nebo v případě, že osoba podezřelá z trestného činu nebo se třetí osoba věci zbavila, nebo byla věc vydána dobrovolně (pokud jde o osobní údaje, věci se zbavila nebo věc vydala samotná dotčená fyzická osoba) ([208]). Nezákonné prohlídky a zajištění věci podléhají trestním sankcím ([209]) a jakýkoli důkaz získaný v rozporu se zákonem o trestním řízení je považován za nepřípustný ([210]). A konečně musí být dotčené osoby o prohlídce nebo zajištění věci (včetně zajištění jejich údajů) vždy bezodkladně informovány ([211]), což následně usnadní výkon hmotných práv fyzické osoby a práva na nápravu (viz zejména možnost vznést námitku proti výkonu příkazu k zajištění věci, viz 180. bod odůvodnění).

3.2.1.2 Přístup k údajům o komunikaci

(155) Podle zákona o ochraně důvěrnosti komunikací mohou korejské orgány činné v trestním řízení přijmout dva druhy opatření ([212]): na jedné straně shromažďování „údajů potvrzujících komunikaci“ ([213]), které zahrnují datum telekomunikace, čas zahájení a ukončení, počet odchozích a příchozích hovorů, stejně jako číslo druhého účastníka, četnost použití, protokoly o používání telekomunikačních služeb a informace o poloze (např. z přenosových věží, které přijímají signály); a na druhé straně „opatření omezující komunikaci“, která zahrnují jak shromažďování obsahu klasické pošty, tak přímé odposlechy obsahu telekomunikace ([214]).

(156) K údajům potvrzujícím komunikaci lze získat přístup pouze v případě, že je to nezbytné k provedení trestního vyšetřování nebo k výkonu trestu ([215]), a to na základě soudního příkazu ([216]). V tomto ohledu zákon o ochraně důvěrnosti komunikací vyžaduje, aby byly podrobné informace uvedeny jak v návrhu na vydání příkazu (např. o důvodech návrhu, vztahu k cíli/účastníkovi a nezbytných údajích), tak v soudním příkazu samotném (např. o účelu, cíli a rozsahu opatření) ([217]). Shromažďování údajů bez soudního příkazu se může uskutečnit pouze

([205]) Ustanovení čl. 215 odst. 1 a 2 a článek 113 zákona o trestním řízení. Pro podání návrhu na vydání soudního příkazu musí dotčený orgán předložit materiály prokazující důvody pro podezření určité osoby ze spáchání trestného činu, nezbytnost prohlídky, kontroly nebo zajištění věci a existenci příslušných věcí, které mají být zajištěny (čl. 108 odst. 1 trestního řádu). Soudní příkaz musí mimo jiné uvádět jména osoby podezřelé z trestného činu a daný trestný čin; místo, osobu nebo věci, které mají být prohledány, nebo věci, které mají být zajištěny; datum vystavení a lhůtu platnosti příkazu (čl. 114 odst. 1 ve spojení s článkem 219 zákona o trestním řízení). Viz příloha II oddíl 2.2.1.2.

([206]) Tj. pokud nelze získat soudní příkaz z důvodu naléhavosti na místě činu (čl. 216 odst. 3 zákona o trestním řízení), v takovém případě musí být soudní příkaz neprodleně získán následně (čl. 216 odst. 3 zákona o trestním řízení).

([207]) Ustanovení čl. 216 odst. 1 a 2 zákona o trestním řízení.

([208]) Článek 218 zákona o trestním řízení. Kromě toho, jak je vysvětleno v oddíle 2.2.1.2 přílohy II, dobrovolně vydané věci jsou připuštěny jako důkaz v soudním řízení pouze za předpokladu, že neexistují rozumné pochybnosti o dobrovolnosti zpřístupnění, kterou musí prokázat státní zástupce.

([209]) Článek 321 trestního zákona.

([210]) Článek 308-2 zákona o trestním řízení. Kromě toho může být daná fyzická osoba (a její právní zástupce) přítomna výkonu příkazu k prohlídce nebo zajištění, a může proto vznést námitku v době výkonu příkazu (články 121 a 219 zákona o trestním řízení).

([211]) Články 121 a 122 zákona o trestním řízení (pokud jde o prohlídky) a článek 219 ve spojení s čl. 106 odst. 4 zákona o trestním řízení (pokud jde o zajištění věci).

([212]) Viz také příloha II oddíl 2.2.2.1. Taková opatření mohou být přijata s nařízenou součinností poskytovatelů telekomunikačních služeb, kterým bude předloženo písemné povolení soudu (čl. 9 odst. 2 zákona o ochraně soukromí v komunikacích), které si tyto subjekty musí uchovávat (článek 15-2 zákona o ochraně důvěrnosti komunikací a článek 12 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací). Poskytovatelé telekomunikačních služeb mohou součinnost odmítnout, pokud jsou údaje o cílové osobě uvedené v písemném souhlasu soudu (například telefonní číslo osoby) nesprávné, a za všech okolností mají zakázáno sdělit hesla používaná pro telekomunikaci (čl. 9 odst. 4 zákona o ochraně důvěrnosti komunikací).

([213]) Ustanovení čl. 2 odst. 11 zákona o ochraně důvěrnosti komunikací.

([214]) Viz čl. 2 odst. 6 zákona o ochraně důvěrnosti komunikací, který se týká „cenzury“ (otevírání pošty bez souhlasu dotčené strany nebo získávání poznatků, pořizování záznamů nebo zadržování obsahu pošty jinými prostředky), a čl. 2 odst. 7 zákona o ochraně důvěrnosti komunikací, který se týká „odposlechu“ (získávání nebo nahrávání obsahu telekomunikace poslechem nebo souběžným odečítáním zvuků, slov, symbolů nebo obrazů v rámci komunikace prostřednictvím elektronických a mechanických zařízení bez souhlasu zúčastněné strany nebo rušení jejich přenosu a příjmu).

([215]) Ustanovení čl. 13 odst. 1 zákona o ochraně důvěrnosti komunikací. Viz také příloha II oddíl 2.2.2.3. Kromě toho lze údaje o sledování polohy v reálném čase a údaje potvrzující komunikaci, které se týkají konkrétní základnové stanice, shromažďovat pouze pro účely vyšetřování závažných trestných činů nebo v situaci, kdy by bylo jinak obtížné zabránit trestnému činu nebo shromáždit důkazy (čl. 13 odst. 2 zákona o ochraně důvěrnosti komunikací). To odráží potřebu poskytnout další záruky v případě opatření, která zvláště narušují soukromí, v souladu se zásadou proporcionality.

([216]) Články 13 a 6 zákona o ochraně důvěrnosti komunikací.

([217]) Viz čl. 13 odst. 3 a 9 ve spojení s čl. 6 odst. 4 a 6 zákona o ochraně důvěrnosti komunikací.

v případě, že naléhavé důvody znemožňují získat souhlas soudu, a v takovém případě musí být soudní příkaz získán a sdělen poskytovateli telekomunikačních služeb ihned po vyžádání údajů ([218]). Pokud soud odmítne udělit následné povolení, musí být shromážděné údaje zničeny ([219]).

(157) Pokud jde o další záruky týkající se shromažďování údajů potvrzujících komunikaci, zákon o ochraně důvěrnosti komunikací ukládá zvláštní požadavky na vedení záznamů a transparentnost ([220]). Orgány činné v trestním řízení ([221]) a poskytovatelé telekomunikačních služeb ([222]) musí zejména vést záznamy o návrzích a zpřístupněních. Kromě toho musí orgány činné v trestním řízení zásadně informovat fyzické osoby o tom, že byly shromážděny jejich údaje potvrzující komunikaci ([223]). Toto oznámení lze odložit pouze ve výjimečných případech na základě souhlasu ředitele příslušného okresního úřadu státního zastupitelství ([224]). Tento souhlas lze vydat pouze v případě, že by oznámení mohlo 1) ohrozit národní bezpečnost, veřejnou bezpečnost a pořádek; 2) způsobit smrt nebo újmu na zdraví; 3) bránit spravedlivému soudnímu řízení (např. vést ke zničení důkazů nebo k vyhrožování svědkům) nebo 4) hanobit podezřelého, oběti nebo jiné osoby související s případem nebo narušit jejich soukromí. V těchto případech musí být oznámení podáno do 30 dnů, jakmile pominou důvody odkladu ([225]). Po oznámení mají fyzické osoby právo získat informace o důvodech shromažďování jejich údajů ([226]).

(158) Přísnější pravidla se vztahují na opatření omezující komunikaci, která lze použít pouze za předpokladu, že existuje závažný důvod k podezření, že jsou plánovány, páchány nebo spáchány některé závažné trestné činy konkrétně vyjmenované v zákoně o ochraně důvěrnosti komunikací ([227]). Kromě toho lze opatření omezující komunikaci přijmout pouze jako poslední možnost a pouze v případě, že je obtížné jinak zabránit spáchání trestného činu, zatknout pachatele trestné činnosti nebo shromáždit důkazy ([228]). Jakmile již tato opatření nejsou nezbytná, musí být okamžitě ukončena, aby se zajistilo, že narušení důvěrnosti komunikací bude co nejmenší ([229]). Údaje, které byly získány nezákonně za pomoci opatření omezujících komunikaci, nebudou uznány jako důkaz v soudním nebo disciplinárním řízení ([230]).

(159) Pokud jde o procesní záruky, zákon o ochraně důvěrnosti komunikací vyžaduje, aby byl získán soudní příkaz k provedení opatření omezujících komunikaci ([231]). Zákon o ochraně důvěrnosti komunikací opět vyžaduje, aby návrh na vydání soudního příkazu a samotný soudní příkaz obsahovaly podrobné údaje ([232]), včetně odůvodnění návrhu, a rovněž komunikaci, jež má být shromážděna (která musí být komunikací vyšetřované podezřelé osoby) ([233]). Tato opatření mohou být bez soudního příkazu přijata pouze v případě bezprostřední hrozby organizované trestné činnosti nebo jiného závažného trestného činu, který může přímo způsobit smrt nebo

([218]) Ustanovení čl. 13 odst. 2 zákona o ochraně důvěrnosti komunikací.
([219]) Ustanovení čl. 13 odst. 3 zákona o ochraně důvěrnosti komunikací.
([220]) Viz příloha II oddíl 2.2.2.3.
([221]) Ustanovení čl. 13 odst. 5 a 6 zákona o ochraně důvěrnosti komunikací.
([222]) Ustanovení čl. 13 odst. 7 zákona o ochraně důvěrnosti komunikací. Kromě toho musí poskytovatelé telekomunikačních služeb dvakrát ročně předložit ministerstvu pro vědu a IKT zprávu o zpřístupnění údajů potvrzujících komunikaci.
([223]) Viz čl. 13-3 odst. 7 ve spojení s článkem 9-2 zákona o ochraně důvěrnosti komunikací. Konkrétně musí být fyzické osoby informovány do 30 dnů poté, co je přijato rozhodnutí (ne)vést trestní stíhání, nebo do 30 dnů po jednom roce od přijetí rozhodnutí o pozastavení obžaloby (oznámení však musí být v každém případě poskytnuto do 30 dnů po jednom roce po shromáždění informací), viz čl. 13-3 odst. 1 zákona o ochraně důvěrnosti komunikací.
([224]) Ustanovení čl. 13-3 odst. 2 a 3 zákona o ochraně důvěrnosti komunikací.
([225]) Ustanovení čl. 13-3 odst. 4 zákona o ochraně důvěrnosti komunikací.
([226]) Ustanovení čl. 13-3 odst. 5 zákona o ochraně důvěrnosti komunikací. Na žádost fyzické osoby musí státní zástupce nebo příslušník soudní policie písemně uvést důvody do 30 dnů od obdržení žádosti, pokud se nepoužije některá z výjimek pro odklad oznámení (čl. 13-3 odst. 6 zákona o ochraně důvěrnosti komunikací).
([227]) Například povstání, trestné činy související s drogami nebo trestné činy zahrnující výbušniny, jakož i trestné činy související s národní bezpečností, diplomatickými vztahy nebo vojenskými základnami a zařízeními, viz čl. 5 odst. 1 zákona o ochraně důvěrnosti komunikací. Viz také příloha II oddíl 2.2.2.2.
([228]) Ustanovení čl. 3 odst. 2 a čl. 5 odst. 1 zákona o ochraně důvěrnosti komunikací.
([229]) Článek 2 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([230]) Článek 4 zákona o ochraně důvěrnosti komunikací.
([231]) Ustanovení čl. 6 odst. 1, 2, 5 a 6 zákona o ochraně důvěrnosti komunikací.
([232]) Návrh na vydání soudního příkazu musí zejména uvádět 1) podstatné (*prima facie*) důvody pro podezření, že je plánován, je páchán nebo byl spáchán jeden z vyjmenovaných trestných činů, a rovněž veškeré podpůrné materiály; 2) opatření omezující komunikaci, jakož i jejich cíl, rozsah, účel a dobu účinnosti a 3) místo, kde by byla opatření provedena, a způsob, jakým by byla provedena (čl. 6 odst. 4 zákona o ochraně důvěrnosti komunikací a čl. 4 odst. 1 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací). Soudní příkaz sám musí specifikovat daná opatření a také jejich cíl, rozsah, dobu účinnosti, místo provedení a způsob, jakým budou opatření prováděna (čl. 6 odst. 6 zákona o ochraně důvěrnosti komunikací).
([233]) Cílem opatření omezujícího komunikaci musí být konkrétní poštovní zásilky nebo telekomunikační sdělení odeslané nebo přijaté podezřelou osobou nebo poštovní zásilky nebo telekomunikační sdělení odeslané nebo přijaté podezřelou osobou během pevně stanoveného časového období (čl. 5 odst. 2 zákona o ochraně důvěrnosti komunikací).

vážnou újmu na zdraví, pokud nastane mimořádná situace, která znemožní uplatnit celý řádný postup ([234]). V takovém případě však musí být návrh na vydání soudního příkazu podán ihned po přijetí opatření ([235]). Opatření omezující komunikaci lze provádět nejvýše po dobu dvou měsíců ([236]) a lze je prodloužit pouze se souhlasem soudu, pokud jsou nadále splněny podmínky pro provedení opatření ([237]). Prodloužená lhůta nesmí celkově překročit jeden rok nebo tři roky v případě některých zvláště závažných trestných činů (např. trestných činů souvisejících s povstáním, zahraniční agresí, národní bezpečností atd.) ([238]).

(160) Stejně jako v případě shromažďování údajů potvrzujících komunikaci zákon o ochraně důvěrnosti komunikací vyžaduje, aby poskytovatelé telekomunikačních služeb ([239]) a donucovací orgány ([240]) vedli záznamy o provedení opatření omezujících komunikaci, a stanoví povinnost informování dotčené fyzické osoby, které lze výjimečně v případě potřeby odložit z důležitých důvodů veřejného zájmu ([241]).

(161) A konečně nedodržení více omezení a záruk podle zákona o ochraně důvěrnosti komunikací (včetně například povinností získat soudní příkaz, vést záznamy a informovat fyzickou osobu), a to s ohledem na shromažďování údajů potvrzujících komunikaci i na použití opatření omezujících komunikaci, podléhá trestním sankcím ([242]).

(162) Pravomoci orgánů činných v trestním řízení shromažďovat komunikační údaje na základě zákona o ochraně důvěrnosti komunikací (obsah komunikace i údaje potvrzující komunikaci) jsou proto vymezeny jasnými a přesnými pravidly a vztahuje se na ně řada záruk. Tyto záruky zejména zaručují dozor nad prováděním takových opatření, a to jak *ex ante* (prostřednictvím předchozího souhlasu soudu), tak *ex post* (prostřednictvím vedení záznamů a požadavků na podávání zpráv), a usnadňují fyzickým osobám přístup k účinným opravným prostředkům (neboť zajišťují, aby byly fyzické osoby informovány o shromažďování jejich údajů).

3.2.1.3 Žádosti o dobrovolné zpřístupnění údajů účastníků

(163) Kromě toho, že se korejské donucovací orgány opírají o povinná opatření popsaná ve 153. až 162. bodě odůvodnění, mohou požádat poskytovatele telekomunikačních služeb o dobrovolné zpřístupnění „komunikačních údajů“ na podporu trestního řízení, vyšetřování nebo výkonu trestu (čl. 83 odst. 3 zákona o telekomunikačních službách). Tato možnost se týká pouze omezených datových souborů, tzn. jméno, registrační číslo rezidenta, adresa a telefonní číslo uživatelů, data, kterými se uživatelé přihlásí k odběru služby nebo jej ukončí, a identifikační kódy uživatelů (tj. kódy používané k identifikaci oprávněného uživatele počítačových systémů nebo komunikačních sítí) ([243]). Vzhledem k tomu, že za „uživatele“ ([244]) jsou považovány pouze fyzické osoby, které přímo objednávají služby od korejského poskytovatele telekomunikačních služeb, fyzické osoby z EU, jejichž údaje byly předány Korejské republice, by obvykle do této kategorie nespadaly ([245]).

(164) Pro taková dobrovolná zpřístupnění platí různá omezení, a to jak s ohledem na výkon pravomocí donucovacího orgánu, tak na reakci poskytovatele telekomunikačních služeb. Obecně musí donucovací orgány jednat v souladu s ústavními zásadami nezbytnosti a proporcionality (čl. 12 odst. 1 a čl. 37 odst. 2 ústavy), a to i tehdy, když žádají o dobrovolné zpřístupnění údajů. Kromě toho musí dodržovat zákon o ochraně osobních údajů, zejména tím, že shromažďují pouze minimální objem osobních údajů v rozsahu nezbytném k dosažení legitimního

([234]) Ustanovení čl. 8 odst. 1 zákona o ochraně důvěrnosti komunikací. Shromažďování údajů v mimořádných situacích však musí vždy probíhat v souladu s „prohlášením o mimořádné cenzuře/odposlechu“ a orgán provádějící shromažďování musí vést registr všech mimořádných opatření (čl. 8 odst. 4 zákona o ochraně důvěrnosti komunikací).

([235]) Shromažďování musí být okamžitě zastaveno, pokud donucovací orgán nezíská soudní povolení do 36 hodin (čl. 8 odst. 2 zákona o ochraně důvěrnosti komunikací), v takovém případě, jak je vysvětleno v oddíle 2.2.2.2 přílohy II, budou shromážděné informace v zásadě zničeny. Soud musí být rovněž informován v případě, že mimořádná opatření byla provedena v tak krátké době, že nebylo nutné získat povolení (např. pokud je podezřelá osoba zatčena ihned po zahájení odposlechu, viz čl. 8 odst. 5 zákona o ochraně důvěrnosti komunikací). V takovém případě musí být soudu poskytnuty informace o účelu, cíli, rozsahu, době, místě provedení a způsobu shromažďování údajů, jakož i důvody pro nepodání žádosti o povolení soudu (čl. 8 odst. 6 až 7) zákona o ochraně důvěrnosti komunikací).

([236]) Ustanovení čl. 6 odst. 7 zákona o ochraně důvěrnosti komunikací. Je-li cíle opatření dosaženo dříve v této lhůtě, musí být opatření okamžitě ukončena.

([237]) Ustanovení čl. 6 odst. 7 a 8 zákona o ochraně důvěrnosti komunikací.

([238]) Ustanovení čl. 6 odst. 8 zákona o ochraně důvěrnosti komunikací.

([239]) Ustanovení čl. 9 odst. 3 zákona o ochraně důvěrnosti komunikací.

([240]) Ustanovení čl. 18 odst. 1 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.

([241]) Státní zástupce musí zejména fyzickou osobu vyrozumět do 30 dnů od vydání obžaloby nebo rozhodnutí neobviňovat nebo nezadržovat příslušnou osobu (čl. 9-2 odst. 1 zákona o ochraně důvěrnosti komunikací). Oznámení lze odložit se souhlasem vedoucího okresního státního zastupitelství, pokud je pravděpodobné, že by vážně ohrozilo národní bezpečnost nebo narušilo veřejnou bezpečnost a pořádek, nebo pokud by pravděpodobně způsobilo podstatnou újmu na životech a zdraví jiných osob (čl. 9-2 odst. 4 až 6 zákona o ochraně důvěrnosti komunikací).

([242]) Články 16 a 17 zákona o ochraně důvěrnosti komunikací.

([243]) Ustanovení čl. 83 odst. 3 zákona o telekomunikačních službách. Viz také příloha II oddíl 2.2.3.

([244]) Ustanovení čl. 2 odst. 9 zákona o telekomunikačních službách.

([245]) Viz také příloha II oddíl 2.2.3.

účelu, a to tak, aby minimalizovaly dopad na soukromí jednotlivců (např. čl. 3 odst. 1 a 6 zákona o ochraně osobních údajů). Konkrétně musí být žádosti o získání komunikačních údajů na základě zákona o telekomunikačních službách podány písemně a musí uvádět důvody žádosti, odkaz na příslušného uživatele a rozsah požadovaných údajů ([246]).

(165) Poskytovatelé telekomunikačních služeb nejsou povinni těmto požadavkům vyhovět a mohou tak učinit pouze v souladu se zákonem o ochraně osobních údajů. To zejména znamená, že musí vyvážit různé dotčené zájmy a nesmí poskytovat údaje, pokud by to pravděpodobně nekorektním způsobem narušilo zájmy dané fyzické osoby nebo třetí strany ([247]). Tak by tomu bylo například v případě, kdy je zřejmé, že dožadující orgán zneužil své pravomoci ([248]). Poskytovatelé telekomunikačních služeb musí vést záznamy o zpřístupněních podle zákona o telekomunikačních službách a dvakrát ročně podávat zprávy ministrovi pro vědu a IKT ([249]).

(166) Kromě toho v souladu s oddílem 3 oznámení č. 2021-5 (příloha I) musí poskytovatelé telekomunikačních služeb zpravidla vyrozumět dotčenou fyzickou osobu, pokud určité žádosti vyhoví dobrovolně ([250]). To pak fyzické osobě umožní uplatnit její práva a v případě, že jsou její údaje zpřístupněny nezákonně, získat ochranu, a to buď vůči správci (například za zpřístupnění údajů v rozporu se zákonem o ochraně osobních údajů nebo za odpověď na žádost, jež byla zjevně nepřiměřená), nebo vůči donucovacímu orgánu (například za jednání nad rámec toho, co je nezbytné a přiměřené, nebo za nedodržení procesních požadavků zákona o telekomunikačních službách).

3.2.2 *Další použití shromážděných informací*

(167) Zpracování osobních údajů shromážděných korejskými orgány činnými v trestním řízení podléhá všem požadavkům zákona o ochraně osobních údajů, včetně požadavků týkajících se účelového omezení (čl. 3 odst. 1 až 2 zákona o ochraně osobních údajů), zákonnosti použití a poskytování třetím stranám (články 15, 17 a 18 zákona o ochraně osobních údajů), mezinárodních předání (články 17 a 18 zákona o ochraně osobních údajů ve spojení s oddílem 2 oznámení č. 2021-5) ([251]), proporcionality/minimalizace údajů (čl. 3 odst. 1 a 6 zákona o ochraně osobních údajů) a omezení uložení (článek 21 zákona o ochraně osobních údajů) ([252]).

(168) Pokud jde o obsah komunikace získaný při provádění opatření omezujících komunikaci, zákon o ochraně důvěrnosti komunikací konkrétně omezuje jejich možné použití na vyšetřování, trestní stíhání nebo prevenci závažné trestné činnosti ([253]); disciplinární řízení pro tytéž trestné činy; nároky na náhradu škody podané jednou ze stran komunikace, nebo pokud to specificky umožňují jiné právní předpisy ([254]). Shromážděný obsah telekomunikace přenášený prostřednictvím internetu lze navíc uchovávat pouze se souhlasem soudu, který opatření omezující komunikaci povolil ([255]), a to za účelem jeho použití pro vyšetřování, trestní stíhání nebo prevenci závažné trestné činnosti ([256]). Obecněji zákon o ochraně důvěrnosti komunikací zakazuje zveřejňování důvěrných údajů získaných pomocí opatření omezujících komunikaci a používání takových údajů k poškození pověsti osob, na které se opatření vztahovala ([257]).

3.2.3 *Dozor*

(169) Dozor nad činností orgánů činných v trestním řízení v Koreji zajišťují různé subjekty ([258]).

([246]) Ustanovení čl. 83 odst. 4 zákona o telekomunikačních službách. Není-li možné z důvodu naléhavosti podat písemnou žádost, musí být písemná žádost podána, jakmile pomine důvod této naléhavosti (čl. 83 odst. 4 zákona o telekomunikačních službách).
([247]) Ustanovení čl. 18 odst. 2 zákona o ochraně osobních údajů.
([248]) Rozhodnutí Nejvyššího soudu 2012Da105482, 10. března 2016. Toto rozhodnutí Nejvyššího soudu viz také příloha II oddíl 2.2.3.
([249]) Ustanovení čl. 83 odst. 5 a 6 zákona o telekomunikačních službách.
([250]) Tento požadavek podléhá omezeným a kvalifikovaným výjimkám, zejména pokud a dokud by oznámení ohrozilo probíhající vyšetřování trestného činu nebo by pravděpodobně způsobilo újmu na životě či zdraví jiné osoby, přičemž tato práva nebo zájmy jsou zjevně nadřazeny právům subjektu údajů. Viz oddíl 3 bod iii) podbod 1 oznámení.
([251]) Korejské orgány veřejné správy jsou zejména povinny prostřednictvím právně závazného nástroje zajistit úroveň ochrany rovnocennou zákonu o ochraně osobních údajů, viz rovněž 90. bod odůvodnění).
([252]) Viz také příloha II oddíl 1.2.
([253]) Viz 158. bod odůvodnění.
([254]) Článek 12 zákona o ochraně důvěrnosti komunikací. Viz příloha II oddíl 2.2.2.2.
([255]) Státní zástupce nebo policista provádějící opatření omezující komunikaci musí do 14 dnů po skončení opatření vybrat telekomunikační údaje, které mají být uchovány, a požádat o souhlas soudu (v případě návrhu policie musí být žádost podána státnímu zástupci, který následně předloží žádost soudu), viz čl. 12-2 odst. 1 a 2 zákona o ochraně důvěrnosti komunikací.
([256]) Žádost o takové povolení musí obsahovat informace o opatřeních omezujících komunikaci, souhrn výsledků opatření, důvody uchovávání (spolu s podpůrnými materiály) a telekomunikační údaje, které mají být uchovány (čl. 12-2 odst. 3 zákona o ochraně důvěrnosti komunikací). Není-li podána žádná žádost, získané údaje musí být vymazány do čtrnácti dnů po skončení opatření omezujícího komunikaci (čl. 12-2 odst. 5 zákona o ochraně důvěrnosti komunikací), a pokud je žádost zamítnuta, do sedmi dnů (čl. 12-2 odst. 5 zákona o ochraně důvěrnosti komunikací. V obou případech je třeba do sedmi dnů podat zprávu o výmazu soudu, který shromažďování údajů povolil.
([257]) Ustanovení čl. 11 odst. 2 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([258]) Viz příloha II oddíl 2.3.

(170) Zaprvé policie podléhá vnitřnímu dozoru ze strany generálního inspektora ([259]), který provádí kontrolu zákonnosti, včetně možného porušování lidských práv. Funkce generálního inspektora byla zřízena k provedení zákona o auditu ve veřejném sektoru, který podporuje zřizování subjektů pro vlastní audit a stanoví konkrétní požadavky na jejich složení a úkoly. Zákon zejména vyžaduje, aby byl vedoucí orgánu vlastního auditu jmenován z řad osob mimo daný orgán (např. bývalí soudci, profesoři) na dobu dvou až pěti let ([260]), tohoto vedoucího pracovníka lze odvolat pouze z oprávněných důvodů (např. nemůže vykonávat své povinnosti ze zdravotních důvodů nebo mu je uloženo disciplinární opatření) ([261]) a je zaručena jeho maximální možná nezávislost ([262]). Mařením vlastního auditu podléhá správním pokutám ([263]). Zprávy o auditu (které mohou zahrnovat doporučení, žádosti o disciplinární opatření a žádosti o odškodnění nebo opravu) jsou předávány vedoucímu pracovníkovi příslušného orgánu veřejné správy, Radě pro audit a inspekce ([264]) a jsou obvykle zveřejňovány ([265]). Výsledky provedení zprávy musí být rovněž oznámeny Radě pro audit a inspekce ([266]) (dozorová úloha a pravomoci Rady pro audit a inspekce viz 173. bod odůvodnění).

(171) Zadruhé Komise pro ochranu osobních údajů dohlíží na soulad zpracování údajů, které provádějí orgány činné v trestním řízení, se zákonem o ochraně osobních údajů a dalšími právními předpisy, které chrání soukromí jednotlivců, včetně právních předpisů upravujících shromažďování (elektronických) důkazů pro účely prosazování trestního práva, jak je popsáno v oddíle 3.2.1 ([267]). Zejména vzhledem k tomu, že se dozor Komise pro ochranu osobních údajů vztahuje na zákonnost a spravedlnost shromažďování a zpracování údajů (čl. 3 odst. 1 zákona o ochraně osobních údajů), k jejichž porušení dojde v případě přístupu k osobním údajům a jejich použití v rozporu s těmito právními předpisy ([268]), Komise pro ochranu osobních údajů může rovněž vyšetřovat a vynucovat dodržování omezení a záruk popsaných v oddíle 3.2.1 ([269]). Při výkonu této dozorové úlohy může Komise pro ochranu osobních údajů využít všech svých vyšetřovacích a nápravných pravomocí, podrobně popsaných v oddíle 2.4.2. Již před nedávnou reformou zákona o ochraně osobních údajů (tzn. v rámci své předchozí dozorové úlohy ve veřejném sektoru) vykonávala Komise pro ochranu osobních údajů několik dozorových činností týkajících se zpracování osobních údajů orgány činnými v trestním řízení, např. v souvislosti s výslechy podezřelých osob (věc č. 2013-16, 26. srpna 2013), s poskytováním oznámení fyzickým osobám o uložení správních pokut (věc č. 2015-02-04, 26. ledna 2015), se sdílením údajů s ostatními orgány (věc č. 2018-15-146, 9. července 2018, věc č. 2018-25-308, 10. prosince 2018; věc č. 2019-02-015, 29. ledna 2019), se shromažďováním otisků prstů nebo fotografií (věc č. 2019-17-273, 9. září 2019) a s používáním dronů (věc č. 2020-01-004, 13. ledna 2020). V těchto případech Komise pro ochranu osobních údajů šetřila soulad s několika ustanoveními zákona o ochraně osobních údajů (např. zákonnost zpracování, zásady účelového omezení a minimalizace údajů), ale také s relevantními ustanoveními jiných právních předpisů, například zákona o trestním řízení, a v případě potřeby vydávala doporučení, aby zajistila soulad zpracování s požadavky na ochranu údajů.

(172) Zatřetí zajišťuje nezávislý dozor Národní komise pro lidská práva ([270]), která může vyšetřovat porušování práv na soukromí a důvěrnost korespondence v rámci svého obecného mandátu chránit základní práva podle článků 10 až 22 ústavy. Národní komise pro lidská práva se skládá z jedenácti komisařů, kteří musí splňovat specifické kvalifikační požadavky ([271]) a jsou jmenováni prezidentem v souladu se zákonem stanovenými postupy. Konkrétně jsou čtyři komisaři jmenováni na návrh Národního shromáždění, čtyři na návrh prezidenta a tři na návrh předsedy Nejvyššího soudu ([272]). Předsedu jmenuje prezident z řad komisařů a musí jej potvrdit Národní shromáždění ([273]). Komisaři (včetně předsedy) jsou jmenováni na tříleté funkční období, které lze prodloužit,

([259]) Viz příloha II oddíl 2.3.1. Viz rovněž https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) Obdobně jsou auditoři jmenováni na základě zvláštních podmínek stanovených zákonem, viz článek 16 a násl. zákona o auditech ve veřejném sektoru.
([261]) Články 8 až 11 zákona o auditech ve veřejném sektoru.
([262]) Článek 7 zákona o auditech ve veřejném sektoru.
([263]) Článek 41 zákona o auditech ve veřejném sektoru.
([264]) Ustanovení čl. 23 odst. 1 zákona o auditech ve veřejném sektoru.
([265]) Článek 26 zákona o auditech ve veřejném sektoru.
([266]) Ustanovení čl. 23 odst. 3 zákona o auditech ve veřejném sektoru.
([267]) Viz čl. 7-8 odst. 3 a 4 a čl. 7-9 odst. 5 zákona o ochraně osobních údajů.
([268]) Viz oznámení Komise pro ochranu osobních údajů č. 2021-5, oddíl 6 (příloha I).
([269]) Viz také příloha II oddíl 2.3.4.
([270]) Článek 1 zákona o Národní komisi pro lidská práva.
([271]) Aby mohl být jmenován, musí komisař 1) působit alespoň deset let na univerzitě nebo v autorizovaném výzkumném ústavu, a to alespoň jako docent; 2) působit jako soudce, státní zástupce nebo advokát po dobu nejméně deseti let; 3) vykonávat činnosti v oblasti lidských práv po dobu nejméně deseti let (např. pro neziskovou, nevládní organizaci nebo mezinárodní organizaci), nebo 4) být doporučen skupinami občanské společnosti (čl. 5 odst. 3 zákona o Národní komisi pro lidská práva). Kromě toho mají po svém jmenování členové Národní komise pro lidská práva zakázáno vykonávat souběžnou funkci v Národním shromáždění, místních radách nebo v orgánu celostátní nebo místní správy (jako úřední osoba), viz článek 10 zákona o Národní komisi pro lidská práva.
([272]) Ustanovení čl. 5 odst. 1 a 2 zákona o Národní komisi pro lidská práva.
([273]) Ustanovení čl. 5 odst. 5 zákona o Národní komisi pro lidská práva.

a mohou být odvoláni pouze v případě, že jsou odsouzeni k trestu odnětí svobody nebo již nejsou schopni plnit své úkoly z důvodu dlouhodobé fyzické nebo duševní nezpůsobilosti (v takovém případě musí s odvoláním souhlasit dvě třetiny komisařů) ([274]). V rámci vyšetřování může Národní komise pro lidská práva požádat o předložení příslušných materiálů, provádět inspekce a předvolávat fyzické osoby k podání výpovědi ([275]). Pokud jde o nápravné pravomoci, může Národní komise pro lidská práva vydávat (veřejná) doporučení ke zlepšení nebo nápravě konkrétních politik a postupů, na která musí orgány veřejné správy odpovědět navrženým plánem provádění ([276]). Pokud dotčený orgán doporučení neprovede, musí o tom komisi vyrozumět ([277]) a ta může o neprovedení informovat Národní shromáždění a/nebo je zveřejnit. Podle oficiálního prohlášení korejské vlády (oddíl 2.3.5 přílohy II) korejské orgány doporučení Národní komise pro lidská práva obecně dodržují a mají k tomu silnou motivaci, protože provádění doporučení je posuzováno jako součást obecného, průběžného hodnocení v rámci pravomoci úřadu předsedy vlády. Roční údaje o její činnosti ukazují, že Národní komise pro lidská práva aktivně dozoruje činnost orgánů činných v trestním řízení, a to na základě individuálních podnětů nebo v rámci vyšetřování z moci úřední ([278]).

(173) Za čtvrté obecný dozor nad zákonností činnosti orgánů veřejné správy zajišťuje Rada pro audit a inspekce, která zkoumá příjmy a výdaje státu, ale také obecněji dohlíží na dodržování povinností orgánů veřejné správy s cílem zlepšit fungování veřejné správy ([279]). Rada pro audit a inspekce je formálně podřízena prezidentovi Korejské republiky, zachovává si však nezávislé postavení, pokud jde o její povinnosti ([280]). Kromě toho je plně nezávislá, pokud jde o jmenování, propouštění a organizaci jejích zaměstnanců a sestavování rozpočtu ([281]). Rada pro audit a inspekce se skládá z předsedy (jmenovaného prezidentem se souhlasem Národního shromáždění) ([282]) a šesti komisařů (jmenovaných prezidentem na doporučení předsedy) ([283]), kteří musí splňovat specifické požadavky na způsobilost stanovené zákonem ([284]) a mohou být odvoláni pouze v případě obžaloby, odsouzení k trestu odnětí svobody nebo neschopnosti plnit své povinnosti z důvodu dlouhodobé duševní nebo fyzické nezpůsobilosti ([285]). Rada pro audit a inspekce provádí roční obecný audit, může však také provádět konkrétní audity v záležitostech zvláštního zájmu. Při provádění auditu nebo inspekce může Rada pro audit a inspekce požadovat předložení dokumentů a vyžádat si účast fyzických osob ([286]). Rada pro audit a inspekce může vydávat doporučení, požadovat disciplinární opatření nebo podávat trestní oznámení ([287]).

(174) A konečně Národní shromáždění vykonává parlamentní dozor nad orgány veřejné správy prostřednictvím vyšetřování a kontrol ([288]) jejich činnosti ([289]). Může požadovat zpřístupnění dokumentů, předvolávat svědky ([290]), doporučovat nápravná opatření (pokud dojde k závěru, že došlo k nezákonné nebo

([274]) Ustanovení čl. 7 odst. 1 a článku 8 zákona o Národní komisi pro lidská práva.
([275]) Článek 36 zákona o Národní komisi pro lidská práva. V souladu s čl. 6 odst. 7 zákona může být předložení materiálů nebo věcí odmítnuto, pokud by poškodilo utajení ze strany státu, které by mohlo mít podstatný vliv na bezpečnost státu nebo diplomatické vztahy, nebo by představovalo závažnou překážku pro vyšetřování trestné činnosti nebo probíhající soudní řízení. V takových případech si může Komise v případě potřeby vyžádat od vedoucího představitele příslušného úřadu (který musí v dobré víře vyhovět) další informace, je-li to nezbytné ke kontrole toho, zda je odmítnutí poskytnout údaje odůvodněné.
([276]) Ustanovení čl. 25 odst. 1 a 3 zákona o Národní komisi pro lidská práva.
([277]) Ustanovení čl. 25 odst. 4 zákona o Národní komisi pro lidská práva.
([278]) Například v letech 2015 až 2019 obdržela Národní komise pro lidská práva ročně 1 380 až 1 699 podnětů týkajících se orgánů činných v trestním řízení a zabývala se stejně vysokým počtem podnětů (např. vyřizovala 1 546 stížností na policii v roce 2018 a 1 249 stížností v roce 2019); provedla také několik vyšetřování z moci úřední, jak je podrobněji popsáno ve výroční zprávě Národní komise pro lidská práva za rok 2018 (k dispozici na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) a ve výroční zprávě Národní komise pro lidská práva za rok 2019 (k dispozici na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([279]) Články 20 a 24 zákona o Radě pro audit a inspekce. Viz příloha II oddíl 2.3.2.
([280]) Ustanovení čl. 2 odst. 1 zákona o Radě pro audit a inspekce.
([281]) Ustanovení čl. 2 odst. 2 zákona o Radě pro audit a inspekce.
([282]) Ustanovení čl. 4 odst. 1 zákona o Radě pro audit a inspekce.
([283]) Ustanovení čl. 5 odst. 1 a článku 6 zákona o Radě pro audit a inspekce.
([284]) Např. výkon činnosti soudce, státního zástupce nebo advokáta po dobu nejméně deseti let, státního úředníka nebo profesora nebo vyšší funkce na univerzitě po dobu nejméně osmi let nebo nejméně deset let práce ve společnosti kotované na burze nebo v instituci s vládními investicemi (z toho nejméně pět let jako výkonný ředitel), viz článek 7 zákona o Radě pro audit a inspekce. Komisaři mají navíc zakázáno účastnit se politických činností a souběžně zastávat funkce v Národním shromáždění, správních úřadech, organizacích podléhající auditu a inspekci Rady pro audit a inspekce nebo jakýkoli jiný placený úřad nebo funkci (článek 9 zákona o Radě pro audit a inspekce).
([285]) Článek 8 zákona o Radě pro audit a inspekce.
([286]) Viz např. článek 27 zákona o Radě pro audit a inspekce.
([287]) Články 24 a 31 až 35 zákona o Radě pro audit a inspekce.
([288]) Článek 128 zákona o Národním shromáždění a články 2, 3 a 15 zákona o inspekci a vyšetřování ve státní správě. To zahrnuje každoroční inspekce záležitostí státní správy jako celku a vyšetřování konkrétních záležitostí.
([289]) Viz příloha oddíl 2.2.3.
([290]) Ustanovení čl. 10 odst. 1 zákona o inspekci a vyšetřování ve státní správě. Viz rovněž články 128 a 129 zákona o Národním shromáždění.

nekalé činnosti) ([291]) a výsledky svých zjištění může zveřejnit ([292]). Pokud Národní shromáždění požádá, aby byla přijata nápravná opatření (která mohou například zahrnovat přiznání odškodnění, přijetí disciplinárního opatření nebo zlepšení vnitřních postupů), je dotčený orgán veřejné správy povinen neprodleně jednat a o výsledku informovat Národní shromáždění ([293]).

3.2.4 *Opravné prostředky*

(175) Korejský systém nabízí různé (soudní) cesty k dosažení nápravy, včetně náhrady škody.

(176) Zaprvé zákon o ochraně osobních údajů poskytuje fyzickým osobám právo na přístup, opravu, výmaz a pozastavení zpracování, pokud jde o osobní údaje zpracovávané pro účely prosazování trestního práva ([294]).

(177) Zadruhé mohou fyzické osoby využít různé nápravné mechanismy, které nabízí zákon o ochraně osobních údajů, pokud jejich údaje zpracoval orgán činný v trestním řízení v rozporu se zákonem o ochraně osobních údajů nebo v rozporu s omezeními a zárukami upravujícími shromažďování osobních údajů podle jiných právních předpisů (tj. zákona o trestním řízení nebo zákona o ochraně důvěrnosti komunikací, viz 171. bod odůvodnění). Fyzické osoby mohou zejména podat stížnost Komisi pro ochranu osobních údajů (a to i prostřednictvím kontaktního centra pro ochranu soukromí, které provozuje Korejská agentura pro internet a bezpečnost ([295])) nebo u mediačního výboru pro spory týkající se osobních údajů ([296]). Na tyto možnosti dosažení nápravy se nevztahují další požadavky na přípustnost. Podle zákona o správním soudním řízení mohou také fyzické osoby podat opravný prostředek proti rozhodnutím nebo nečinnosti / napadnout rozhodnutí nebo nečinnost Komise pro ochranu osobních údajů (viz 132. bod odůvodnění).

(178) Zatřetí může kterákoli fyzická osoba ([297]) podat stížnost k Národní komisi pro lidská práva, pokud jde o porušení práva na soukromí a ochranu údajů ze strany korejského orgánu činného v trestním řízení. Národní komise pro lidská práva může doporučit nápravu nebo zlepšení jakéhokoli příslušného právního předpisu, instituce, postupu nebo praxe ([298]) nebo provedení nápravných opatření, například mediace ([299]), ukončení porušování lidských práv, náhradu škody a opatření zamezující opakování stejného nebo podobného porušování práv ([300]). Podle oficiálního prohlášení korejské vlády (oddíl 2.4.2 přílohy II) to může zahrnovat také výmaz nezákonně shromážděných osobních údajů. Ačkoli Národní komise pro lidská práva nemá pravomoc vydávat závazná rozhodnutí, nabízí neformálnější, méně nákladný a snadno dostupný způsob nápravy, zejména z toho důvodu, že (jak je vysvětleno v příloze II oddílu 2.4.2) k prošetření stížnosti nevyžaduje prokázání skutečné újmy ([301]). Tím je zajištěno, že stížnosti fyzických osob týkající se shromažďování jejich údajů je možné prošetřit i v případě, že dotčená fyzická osoba nemůže prokázat, že její údaje byly skutečně shromážděny (například proto, že oznámení fyzické osobě dosud nebylo vydáno). Výroční zprávy o činnosti Národní komise pro lidská práva ukazují, že fyzické osoby také v praxi využívají tento způsob napadení činnosti orgánů činných v trestním řízení, a to včetně nakládání s osobními údaji ([302]). Pokud fyzická osoba není s výsledkem řízení u Národní komise pro lidská práva spokojena, může

([291]) Ustanovení čl. 16 odst. 2 zákona o inspekci a vyšetřování ve státní správě.
([292]) Ustanovení čl. 12-2 zákona o inspekci a vyšetřování ve státní správě.
([293]) Ustanovení čl. 16 odst. 3 zákona o inspekci a vyšetřování ve státní správě.
([294]) Toto právo lze uplatňovat přímo vůči příslušnému orgánu nebo nepřímo prostřednictvím Komise pro ochranu osobních údajů (čl. 35 odst. 2 zákona o ochraně osobních údajů). Jak je podrobněji popsáno v 76. až 78. bodě odůvodnění, výjimky z těchto práv se použijí pouze v případě, že je to nezbytné k ochraně důležitých (veřejných) zájmů.
([295]) Článek 62 zákona o ochraně osobních údajů.
([296]) Články 40 až 50 zákona o ochraně osobních údajů a články 48-2 až 57 prováděcí vyhlášky k zákonu o ochraně osobních údajů. Viz také příloha II oddíl 2.4.1.
([297]) Jak vysvětluje příloha II oddíl 2.4.2, ačkoli článek 4 zákona o Národní komisi pro lidská práva uvádí občany a cizince s bydlištěm v Korejské republice, výraz „s bydlištěm" odráží spíše koncepci na základě jurisdikce než území. Pokud tedy vnitrostátní instituce v Koreji poruší základní práva cizího státního příslušníka, může tato osoba podat stížnost Národní komisi pro lidská práva. Tak by tomu bylo v případě, že by k osobním údajům cizího státního příslušníka předaným do Koreje získaly nezákonný přístup korejské orgány veřejné správy. Viz zejména vysvětlení na adrese https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) Článek 44 zákona o Národní komisi pro lidská práva.
([299]) Fyzická osoba může také požádat o řešení stížnosti prostřednictvím mediace, viz článek 42 a násl. zákona o Národní komisi pro lidská práva.
([300]) Ustanovení čl. 42 odst. 4 zákona o Národní komisi pro lidská práva. Navíc může Národní komise pro lidská práva přijmout naléhavá nápravná opatření, pokud porušování práv pokračuje a pokud by nebylo řešeno, pravděpodobně by způsobilo obtížně napravitelnou škodu, viz článek 48 zákona o Národní komisi pro lidská práva.
([301]) Stížnost musí být zpravidla podána do jednoho roku od porušení práv, Národní komise pro lidská práva se však může přesto rozhodnout prošetřit stížnost podanou po této lhůtě, pokud neuplynula promlčecí lhůta podle trestního nebo občanského práva (čl. 32 odst. 1 bod 4 zákona o Národní komisi pro lidská práva).
([302]) Národní komise pro lidská práva například v minulosti řešila stížnosti a vydala doporučení týkající se nezákonných zajištění věcí a porušení povinnosti informovat fyzické osoby o zajištění věci (viz s. 80 a 91 výroční zprávy Národní komise pro lidská práva za rok 2018, k dispozici na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), jakož i nezákonného zpracování osobních údajů ze strany policie, státního zastupitelství a soudů (viz s. 157–158 výroční zprávy Národní komise pro lidská práva za rok 2019, k dispozici na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, a s. 76 výroční zprávy za rok 2019, k dispozici na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

rozhodnutí (například rozhodnutí nepokračovat ve vyšetřování stížnosti ([303])) a doporučení komise napadnout u korejských soudů podle zákona o správním soudním řízení (viz 181. bod odůvodnění) ([304]). Kromě toho může řízení před Národní komisí pro lidská práva dále usnadnit přístup k soudům, protože fyzická osoba by v souladu s postupy popsanými ve 181. až 183. bodě odůvodnění mohla podat další opravný prostředek vůči orgánu veřejné správy, který podle zjištění Národní komise pro lidská práva nezákonně zpracoval osobní údaje této osoby.

(179) A konečně jsou k dispozici různé soudní opravné prostředky, které fyzickým osobám umožňují dovolávat se k dosažení nápravy omezení a záruk popsaných v oddíle 3.2.1 ([305]).

(180) Pokud jde o zajištění věcí (včetně údajů), zákon o trestním řízení stanoví možnost vznést námitku proti výkonu příkazu nebo jej napadnout prostřednictvím „kvazistížnosti“, podáním návrhu u příslušného soudu s žádostí o zrušení nebo změnu opatření, které učinil státní zástupce nebo policista ([306]).

(181) V obecnějším smyslu mohou fyzické osoby napadnout jednání ([307]) nebo opomenutí ([308]) orgánů veřejné správy (včetně orgánů činných v trestním řízení) podle zákona o správním soudním řízení ([309]). Správní opatření se považuje za „napadnutelné opatření“, má-li přímý dopad na občanská práva a povinnosti ([310]), což, jak potvrdila korejská vláda (oddíl 2.4.3 přílohy II), je i případ opatření za účelem shromažďování osobních údajů, ať už přímo (například odposlechem komunikace), prostřednictvím závazných žádostí o zpřístupnění (například poskytovateli služeb) nebo prostřednictvím žádostí o dobrovolnou spolupráci. Aby byla stížnost podle zákona o správním soudním řízení přípustná, musí mít fyzická osoba právní zájem na uplatnění nároku ([311]). Podle judikatury Nejvyššího soudu je „právní zájem“ vykládán jako „právem chráněný zájem“, tj. přímý a konkrétní zájem chráněný právními a správními předpisy, na nichž jsou založena správní opatření (tím se rozumí obecné, nepřímé a abstraktní veřejné zájmy) ([312]). Fyzické osoby mají právní zájem v případě jakéhokoli porušení omezení a záruk týkajících se shromažďování jejich osobních údajů pro účely vymáhání trestního práva (podle zvláštních zákonů nebo zákona o ochraně osobních údajů). Na základě zákona o správním soudním řízení může soud rozhodnout o zrušení nebo změně nezákonného opatření, konstatovat absolutní neplatnost (tj. zjištění, že opatření nemá právní účinky nebo neexistuje v právním řádu) nebo konstatovat, že opomenutí je nezákonné ([313]). Pravomocný rozsudek podle zákona o správním soudním řízení je pro účastníky řízení závazný ([314]).

([303]) Například pokud Národní komise pro lidská práva výjimečně nemůže prověřit určité materiály nebo zařízení, neboť se týkají státních tajemství, která by mohla mít podstatný vliv na bezpečnost státu nebo diplomatické vztahy, nebo by představovala závažnou překážku pro vyšetřování trestné činnosti nebo probíhající soudní řízení, a pokud by to Národní komisi pro lidská práva bránilo provést šetření nezbytné k posouzení podstaty obdržené stížnosti, sdělí fyzické osobě důvody, proč byla stížnost zamítnuta, v souladu s článkem 39 zákona o Národní komisi pro lidská práva. V tomto případě by jednotlivec mohl rozhodnutí Národní komise pro lidská práva napadnout podle zákona o správním soudním řízení.

([304]) Viz např. rozhodnutí Vrchního soudu v Soulu 2007Nu27259, 18. dubna 2008, které potvrdilo rozhodnutí Nejvyššího soudu 2008Du7854, 9. října 2008; rozhodnutí Vrchního soudu v Soulu 2017Nu69382, 2. února 2018.

([305]) Viz příloha II oddíl 2.4.3.

([306]) Článek 417 zákona o trestním řízení ve spojení s čl. 414 odst. 2 zákona o trestním řízení. Viz rozhodnutí Nejvyššího soudu 97Mo66, 29. září 1997.

([307]) Zákon o správním soudním řízení hovoří o „opatření“, tj. o výkonu nebo odmítnutí provést výkon veřejné moci v konkrétním případě.

([308]) Podle zákona o správním soudním řízení se tak označuje dlouhodobá nečinnost správního úřadu, pokud jde o přijetí určitého opatření, v rozporu se zákonnou povinností tak učinit.

([309]) V rámci méně formálního mechanismu nápravy lze správní opravný prostředek uplatnit nejprve u správních odvolacích komisí zřízených při některých orgánech veřejné správy (např. Národní zpravodajské služby, Národní komise pro lidská práva) nebo u Ústřední správní odvolací komise zřízené v rámci Komise pro boj proti korupci a občanská práva (článek 6 zákona o správních opravných prostředcích a čl. 18 odst. 1 zákona o správním soudním řízení). Podle zákona o správním řízení však lze také podat žalobu přímo u korejských soudů.

([310]) Rozhodnutí Nejvyššího soudu 98Du18435, 22. října 1999, rozhodnutí Nejvyššího soudu 99Du1113, 8. září 2000 a rozhodnutí Nejvyššího soudu 2010Du3541, 27. září 2012.

([311]) Články 12, 35 a 36 zákona o správním soudním řízení. Kromě toho musí být návrh na zrušení/změnu opatření a návrh na potvrzení protiprávnosti opomenutí podán do 90 dnů ode dne, kdy se fyzická osoba o opatření/opomenutí dozví, a to zpravidla nejpozději do jednoho roku ode dne, kdy bylo opatření vydáno nebo kdy došlo k opomenutí, pokud neexistují ospravedlnitelné důvody (článek 20 a čl. 38 odst. 2 zákona o správním soudním řízení). Výraz „ospravedlnitelné důvody“ vykládá Nejvyšší soud a je zapotřebí posoudit, zda je společensky přijatelné připustit opožděnou stížnost s ohledem na všechny okolnosti dané věci (rozhodnutí Nejvyššího soudu 90Nu6521, 28. června 1991). Jak potvrzuje korejská vláda v oddíle 2.4.3 přílohy II, zahrnuje to (mimo jiné) důvody prodlení, za které dotčená strana nemůže nést odpovědnost (tj. situace, které jsou mimo kontrolu stěžovatele, například pokud nebyl informován o shromažďování jeho osobních údajů), nebo vyšší moc (např. přírodní katastrofa, válka).

([312]) Rozhodnutí Nejvyššího soudu 2006Du330, 26. března 2006.

([313]) Články 2 a 4 zákona o správním řízení.

([314]) Ustanovení čl. 30 odst. 1 zákona o správním řízení.

(182) Vedle napadení vládních opatření prostřednictvím správní žaloby sporů mohou fyzické osoby podat i ústavní stížnost Ústavnímu soudu, pokud jde o jakékoli porušení jejich základních práv v důsledku výkonu nebo nečinnosti vládní moci (s výjimkou rozsudků soudů) ([315]). Jsou-li k dispozici jiné opravné prostředky, musí být nejprve vyčerpány. Podle judikatury Ústavního soudu mohou cizí státní příslušníci podat ústavní stížnost v rozsahu, v jakém korejská ústava uznává jejich základní práva (viz vysvětlení v oddíle 1.1) ([316]). Ústavní soud může zneplatnit výkon vládní moci, který porušení práva způsobil, nebo potvrdit, že určitá nečinnost je protiústavní ([317]). V takovém případě je příslušný orgán povinen přijmout opatření, aby vyhověl rozhodnutí soudu.

(183) Kromě toho mohou fyzické osoby získat náhradu škody u korejského soudu. To zahrnuje především možnost požadovat odškodnění za porušení zákona o ochraně osobních údajů, kterého se dopustily orgány činné v trestním řízení, a to podle článku 39 (viz také 135. bod odůvodnění). Obecněji řečeno, fyzické osoby mohou žádat o náhradu škody způsobené státními úředníky při výkonu služebních povinností v rozporu se zákonem, a to na základě zákona o náhradě škody státem (viz také 135. bod odůvodnění) ([318]).

(184) Mechanismy popsané ve 176. až 183. bodě odůvodnění poskytují subjektům údajů účinné prostředky správní a soudní ochrany, které jim umožňují zejména výkon jejich práv včetně práva na přístup k jejich osobním údajům nebo na dosažení opravy či výmazu těchto údajů.

3.3 **Přístup korejských orgánů veřejné správy k osobním údajům a jejich použití těmito orgány pro účely národní bezpečnosti**

(185) Právo Korejské republiky ukládá řadu omezení a záruk v oblasti přístupu k osobním údajům a použití těchto údajů pro účely národní bezpečnosti a stanoví dozorové a ochranné mechanismy, které jsou v souladu s požadavky uvedenými ve 141. až 143. bodě odůvodnění tohoto rozhodnutí. Podmínky, za kterých lze takový přístup uskutečnit, a záruky týkající se využívání těchto pravomocí jsou podrobně posouzeny v následujících oddílech.

3.3.1 *Právní základy, omezení a záruky*

(186) V Korejské republice mohou být osobní údaje zpřístupněny pro účely národní bezpečnosti na základě zákona o ochraně důvěrnosti komunikací, zákona o telekomunikačních službách a zákona o boji proti terorismu na ochranu občanů a veřejné bezpečnosti (dále jen „zákon o boji proti terorismu“) ([319]). Hlavním orgánem ([320]) s pravomocemi v oblasti národní bezpečnosti je Národní zpravodajská služba ([321]). Shromažďování a používání osobních údajů Národní zpravodajskou službou musí být v souladu s příslušnými právními požadavky (včetně

([315]) Ustanovení čl. 68 odst. 1 zákona o Ústavním soudu. Ústavní stížnosti musí být podány do 90 dnů poté, co se fyzická osoba dozví o porušení práva, a do jednoho roku poté, co k tomuto porušení práva došlo. Jak je také vysvětleno v příloze II oddíle 2.4.3, vzhledem k tomu, že na řízení podle článku 40 zákona o Ústavním soudu se použije postup podle zákona o správním řízení, bude stížnost přípustná i v případě, že existují „ospravedlnitelné důvody“ ve smyslu výkladu v souladu s judikaturou Nejvyššího soudu popsanou v poznámce pod čarou č. 312. Je-li nejprve nutné vyčerpat jiné opravné prostředky, musí být ústavní stížnost podána do 30 dnů po konečném rozhodnutí o takovém opravném prostředku (článek 69 zákona o Ústavním soudu).

([316]) Rozhodnutí Ústavního soudu 99HeonMa194, 29. listopadu 2001.

([317]) Ustanovení čl. 75 odst. 3 zákona o Ústavním soudu.

([318]) Ustanovení čl. 2 odst. 1 zákona o náhradě škody státem.

([319]) Viz příloha II bod 3.1.

([320]) Výjimečně může policie a státní zastupitelství shromažďovat osobní údaje i pro účely národní bezpečnosti (viz poznámka pod čarou č. 327 a příloha II oddíl 3.2.1.2). Kromě toho má pravomoci v oblasti národní bezpečnosti korejská vojenská zpravodajská služba (Velitelství podpory zabezpečení obrany, zřízené při Ministerstvu obrany). Jak je však vysvětleno v příloze II oddíle 3.1, tato služba odpovídá pouze za vojenské zpravodajství a provádí sledování civilistů pouze v případě, že je to nezbytné pro výkon jejích vojenských funkcí. Vyšetřovat může pouze vojenský personál, civilní zaměstnance armády, osoby ve vojenském výcviku, osoby v armádní záloze nebo náborové službě a válečné zajatce (článek 1 zákona o vojenském soudu). Při shromažďování údajů o komunikaci pro účely národní bezpečnosti podléhá velitelství podpory zabezpečení obrany omezením a zárukám podle zákona o ochraně důvěrnosti komunikací a prováděcí vyhlášky k tomuto zákonu.

([321]) Úkolem Národní zpravodajské služby je shromažďovat, kompilovat a distribuovat informace o jiných zemích (tj. obecné informace o trendech a vývoji týkající se cizích zemí nebo činnosti státních subjektů); zpravodajské informace související s protišpionážní činností (včetně vojenské a průmyslové špionáže), bojem proti terorismu a činnosti mezinárodních syndikátů páchajících trestnou činnost; zpravodajské informace o určitých druzích trestné činnosti namířené proti veřejné a národní bezpečnosti (např. vnitrostátní nepokoje, zahraniční agrese) a zpravodajské informace související se zajišťováním kybernetické bezpečnosti a s předcházením kybernetickým útokům a hrozbám či bojem proti nim (čl. 4 odst. 2 zákona o Národní zpravodajské službě). Viz také příloha II oddíl 3.1.

zákona o ochraně osobních údajů a zákona o ochraně důvěrnosti komunikací) ([322]) a obecnými pokyny, které vypracuje prezident a přezkoumá Národní shromáždění ([323]). Obecně platí, že Národní zpravodajská služba musí zachovávat politickou neutralitu a chránit svobodu a práva jednotlivců ([324]). Pracovníci Národní zpravodajské služby navíc nesmí zneužívat své úřední pravomoci k tomu, aby nutili jakoukoli instituci, organizaci nebo fyzickou osobu činit něco, k čemu nejsou (ze zákona) povinny, ani žádné osobě bránit ve výkonu jejích práv ([325]).

3.3.1.1 Přístup k údajům o komunikaci

(187) Na základě zákona o ochraně důvěrnosti komunikací mohou korejské orgány veřejné správy ([326]) shromažďovat údaje potvrzující komunikaci (tj. datum telekomunikace, čas jejího zahájení a ukončení, počet odchozích a příchozích hovorů a také účastnické číslo druhé strany, četnost použití, protokolové soubory o využití telekomunikačních služeb a údaje o poloze, viz 155. bod odůvodnění) a obsah komunikace (prostřednictvím opatření omezujících komunikaci, viz 155. bod odůvodnění) pro účely národní bezpečnosti (jak je určeno mandátem Národní zpravodajské služby, viz poznámka pod čarou č. 322). Tyto pravomoci se vztahují na dva druhy údajů: 1) komunikace, v nichž jsou jedna nebo obě strany korejskými státními příslušníky ([327]), a 2) komunikace a) zemí nepřátelských vůči Korejské republice; b) zahraničních agentur, skupin nebo státních příslušníků podezřelých z účasti na protikorejských činnostech ([328]) nebo c) členů skupin působících na Korejském poloostrově, ale fakticky mimo oblast svrchovanosti Korejské republiky a jejich zastřešujících skupin se sídlem v zahraničí ([329]). Údaje o komunikaci fyzických osob z EU předané z Unie do Korejské republiky na základě tohoto rozhodnutí lze proto podle zákona o ochraně důvěrnosti komunikací shromažďovat pouze pro účely národní bezpečnosti (s výhradou podmínek stanovených v 188. až 192. bodě odůvodnění), pokud se jedná o komunikaci mezi fyzickou osobou z EU a korejským státním příslušníkem nebo, pokud jde o komunikaci výhradně mezi jinými než korejskými státními příslušníky, jestliže komunikace spadá do jedné ze tří uvedených kategorií 2a), b) a c).

(188) V obou situacích může shromažďování údajů potvrzujících komunikaci probíhat pouze za účelem předcházení hrozbám pro národní bezpečnost ([330]), zatímco opatření omezující komunikaci mohou být přijímána pouze tehdy, existuje-li závažné riziko pro národní bezpečnost a shromažďování údajů je nezbytné k tomu, aby se tomuto riziku předešlo ([331]). Kromě toho lze k obsahu komunikace přistupovat pouze jako k opatření poslední instance a je třeba vyvinout úsilí k minimalizaci narušení důvěrnosti komunikací ([332]) a zajistit tak, aby toto narušení zůstalo přiměřené sledovanému cíli národní bezpečnosti. Shromažďování obsahu komunikace i údajů potvrzujících komunikaci může být prováděno po dobu nejvýše čtyř měsíců, a je-li sledovaného cíle dosaženo dříve, musí být okamžitě ukončeno ([333]). Jsou-li nadále splněny příslušné podmínky, může být lhůta prodloužena s předchozím souhlasem soudu (u opatření popsaných ve 189. bodě odůvodnění) nebo prezidenta (u opatření popsaných ve 190. bodě odůvodnění) ([334]) až o čtyři měsíce.

(189) Tytéž procesní záruky se použijí pro shromažďování údajů potvrzujících komunikaci a obsahu komunikace ([335]). Zejména pokud je alespoň jedna z fyzických osob zapojených do komunikace korejským státním příslušníkem, musí zpravodajská služba předložit písemnou žádost vrchnímu státnímu zastupitelství a v takovém případě pak

([322]) Viz také články 14, 22 a 23 zákona o Národní zpravodajské službě.
([323]) Ustanovení čl. 4 odst. 2 zákona o Národní zpravodajské službě.
([324]) Ustanovení čl. 3 odst. 1, čl. 6 odst. 2, článků 11 a 21 zákona o Národní zpravodajské službě. Viz také pravidla týkající se střetu zájmů, zejména články 10 a 12 zákona o Národní zpravodajské službě.
([325]) Článek 13 zákona o Národní zpravodajské službě.
([326]) To zahrnuje zpravodajské služby (tj. Národní zpravodajskou službu a Velitelství podpory zabezpečení obrany) a policii / státní zastupitelství.
([327]) Ustanovení čl. 7 odst. 1 bodu 1 zákona o ochraně důvěrnosti komunikací.
([328]) Jak vysvětluje korejská vláda v poznámce pod čarou č. 244 přílohy II, jedná se o činnosti, které ohrožují existenci a bezpečnost národa, demokratický řád nebo přežití a svobodu lidí.
([329]) Ustanovení čl. 7 odst. 1 bodu 2 zákona o ochraně důvěrnosti komunikací.
([330]) Článek 13-4 zákona o ochraně důvěrnosti komunikací.
([331]) Ustanovení čl. 7 odst. 1 zákona o ochraně důvěrnosti komunikací.
([332]) Ustanovení čl. 3 odst. 2 zákona o ochraně důvěrnosti komunikací. Kromě toho musí být opatření omezující komunikaci okamžitě ukončena, jakmile již nejsou nezbytná, aby se tak zajistilo, že jakékoli porušení komunikačních tajemství fyzické osoby bude omezeno na minimum (článek 2 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací).
([333]) Ustanovení čl. 7 odst. 2 zákona o ochraně důvěrnosti komunikací.
([334]) Žádost o souhlas s prodloužením opatření týkajících se sledování musí být podána písemně s uvedením důvodů, proč se o prodloužení žádá, a s poskytnutím podpůrných materiálů (čl. 7 odst. 2 zákona o ochraně důvěrnosti komunikací a článek 5 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací).
([335]) Viz čl. 13-4 odst. 2 zákona o ochraně důvěrnosti komunikací a čl. 37 odst. 4 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací, které stanoví, že postupy platné pro shromažďování obsahu komunikace se obdobně použijí na shromažďování údajů potvrzujících komunikaci. Viz také příloha II oddíl 3.2.1.1.1.

musí podat návrh na vydání soudního příkazu předsedovi vrchního soudu ([336]). Zákon o ochraně důvěrnosti komunikací vyjmenovává údaje, které musí být uvedeny v žádosti státnímu zástupci, v návrhu na vydání soudního příkazu a v samotném soudním příkazu, k nimž patří zejména odůvodnění žádosti a hlavní důvody podezření, podpůrné materiály, jakož i údaje o účelu, cíli (tj. cílové osobě / cílových osobách), rozsahu a délce trvání navrhovaného opatření ([337]). Shromažďování údajů bez soudního příkazu může být provedeno pouze v případě, že dojde ke zločinnému spolčení, které ohrožuje národní bezpečnost, a nastane mimořádná událost, kvůli které nelze uskutečnit všechny výše uvedené postupy ([338]). I v takovém případě však musí být návrh na vydání soudního příkazu podán ihned po přijetí opatření ([339]). Zákon o ochraně důvěrnosti komunikací proto jasně vymezuje rozsah a podmínky těchto druhů shromažďování a stanoví pro ně zvláštní (procesní) záruky (včetně předchozího souhlasu soudu), což zajišťuje, že použití takových opatření je omezeno na to, co je nezbytné a přiměřené. Požadavek na poskytnutí podrobných údajů v návrhu na vydání soudního příkazu i v soudním příkazu samotném navíc vylučuje možnost neselektivního přístupu.

(190) V případě komunikace mezi jinými než korejskými státními příslušníky, která spadá do jedné ze tří konkrétních kategorií uvedených ve 187. bodě odůvodnění, je třeba podat žádost řediteli Národní zpravodajské služby, který si po přezkoumání vhodnosti navrhovaných opatření musí vyžádat předchozí písemný souhlas prezidenta Korejské republiky ([340]). Žádost vypracovaná zpravodajskou službou musí obsahovat stejně podrobné údaje jako návrh na vydání soudního příkazu (viz 189. bod odůvodnění), zejména pokud jde o odůvodnění žádosti a hlavní důvody podezření, podpůrné materiály a údaje o účelech, cílové osobě / cílových osobách, rozsahu a době trvání navrhovaných opatření ([341]). V mimořádných situacích ([342]) je třeba získat předchozí souhlas ministra, do jehož gesce náleží příslušná zpravodajská služba, tato zpravodajská služba si však musí vyžádat souhlas prezidenta ihned po přijetí mimořádných opatření ([343]). I v případě shromažďování údajů o komunikaci mezi výhradně jinými než korejskými státními příslušníky tedy zákon o ochraně důvěrnosti komunikací omezuje použití takových opatření na to, co je nezbytné a přiměřené, neboť jasně vymezuje omezené kategorie fyzických osob, které mohou být předmětem takových opatření, a stanoví podrobná kritéria, která musí zpravodajské služby prokázat, aby odůvodnily žádost o shromažďování údajů. To opět vylučuje možnost neselektivního přístupu. Ačkoli neexistuje žádné předchozí nezávislé schválení takových opatření, je nezávislý dozor zajištěn *ex post*, a to ze strany Komise pro ochranu osobních údajů a Národní komise pro lidská práva (viz například 199. a 200. bod odůvodnění).

(191) Zákon o ochraně důvěrnosti komunikací dále ukládá několik dalších záruk, které přispívají k následnému dozoru a usnadňují přístup fyzických osob k účinným opravným prostředkům. Zaprvé, pokud jde o jakýkoli druh shromažďování údajů pro účely národní bezpečnosti, zákon o ochraně důvěrnosti komunikací stanoví různé požadavky na vedení záznamů a podávání zpráv. Konkrétně při žádosti o součinnost soukromých subjektů musí zpravodajské služby předložit soudní příkaz / souhlas prezidenta nebo kopii průvodního dopisu prohlášení o mimořádné cenzuře, které musí dožádaný subjekt uchovat ve své evidenci ([344]). Pokud musí soukromé subjekty poskytnout součinnost, musí dožadující orgán veřejné správy i příslušný subjekt vést záznamy o účelu a předmětu

([336]) Ustanovení čl. 6 odst. 5 a 8 a čl. 7 odst. 1 bod 1 a odst. 3 zákona o ochraně důvěrnosti komunikací ve spojení s čl. 7 odst. 3 a 4 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.

([337]) Viz čl. 7 odst. 3 a čl. 6 odst. 4 zákona o ochraně důvěrnosti komunikací (žádost zpravodajské služby), článek 4 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací (návrh podávaný státním zástupcem) a čl. 7 odst. 3 a čl. 6 odst. 6 zákona o ochraně důvěrnosti komunikací (soudní příkaz).

([338]) Článek 8 zákona o ochraně důvěrnosti komunikací.

([339]) Ustanovení čl. 8 odst. 2 a 8 zákona o ochraně důvěrnosti komunikací. Není-li do 36 hodin od přijetí opatření získán souhlas soudu, musí být shromažďování údajů okamžitě ukončeno. V případech, kdy je sledování dokončeno v krátké době, a není proto možné získat souhlas soudu, musí vedoucí představitel příslušného vrchního státního zastupitelství zaslat oznámení o mimořádném opatření vypracované zpravodajskou službou předsedovi příslušného soudu, který na tomto základě přezkoumá zákonnost shromažďování (čl. 8 odst. 5 a 7 zákona o ochraně důvěrnosti komunikací). V oznámení musí být uveden účel, cíl, rozsah, doba, místo a způsob shromažďování údajů, jakož i důvody pro nepodání žádosti před přijetím opatření (čl. 8 odst. 6 zákona o ochraně důvěrnosti komunikací). Obecněji řečeno, zpravodajské služby mohou přijímat mimořádná opatření pouze v souladu s „prohlášením o mimořádné cenzuře/odposlechu“ a musí vést registr takových opatření (čl. 8 odst. 4 zákona o ochraně důvěrnosti komunikací).

([340]) Ustanovení čl. 8 odst. 1 a 2 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.

([341]) Ustanovení čl. 8 odst. 3 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací ve spojení s čl. 6 odst. 4 zákona o ochraně důvěrnosti komunikací.

([342]) Tj. v případech, kdy je cílem opatření akt spolčení ohrožující národní bezpečnost, není dostatek času na získání souhlasu prezidenta a nepřijetí mimořádných opatření může poškodit národní bezpečnost (čl. 8 odst. 8 zákona o ochraně důvěrnosti komunikací).

([343]) Ustanovení čl. 8 odst. 9 zákona o ochraně důvěrnosti komunikací. Není-li do 36 hodin od podání žádosti získáno povolení, musí být shromažďování údajů okamžitě ukončeno.

([344]) Ustanovení čl. 9 odst. 2 zákona o ochraně důvěrnosti komunikací a článek 12 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací. Možnost nařízení povinné součinnosti pošt a poskytovatelů telekomunikačních služeb viz článek 13 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací. Soukromé subjekty mohou zpřístupnění údajů odmítnout, pokud soudní příkaz / povolení nebo prohlášení o mimořádné cenzuře odkazuje na nesprávný identifikátor (např. telefonní číslo patřící jiné než identifikované osobě). Za žádných okolností nesmí zpřístupňovat hesla používaná pro komunikaci (čl. 9 odst. 4 zákona o ochraně důvěrnosti komunikací).

opatření, jakož i o datu výkonu opatření ([345]). Zpravodajské agentury musí kromě toho řediteli Národní zpravodajské služby oznamovat, jaké údaje shromáždily a jaký je výstup sledování ([346]).

(192) Zadruhé musí být fyzické osoby informovány o shromažďování jejich údajů (údajů potvrzujících komunikaci nebo obsahu komunikace) pro účely národní bezpečnosti, pokud se jedná o komunikaci, v níž je alespoň jedna ze stran korejským státním příslušníkem ([347]). Toto oznámení musí být poskytnuto písemně do 30 dnů ode dne, kdy bylo shromažďování ukončeno (včetně případů, kdy byly údaje získány mimořádným postupem), a lze jej odložit pouze tehdy a na tak dlouho, kdy by ohrozilo národní bezpečnost nebo by znamenalo újmu na životě a fyzické bezpečnosti osob ([348]). Bez ohledu na toto oznámení mohou fyzické osoby dosáhnout nápravy různými prostředky, jak je podrobněji vysvětleno v oddíle 3.3.4.

3.3.1.2 Shromažďování údajů o osobách podezřelých z terorismu

(193) Zákon o boji proti terorismu stanoví, že Národní zpravodajská služba může shromažďovat informace o osobách podezřelých z terorismu ([349]) v souladu s omezeními a zárukami stanovenými v jiných právních předpisech ([350]). Národní zpravodajská služba může zejména získávat komunikační údaje (na základě zákona o ochraně důvěrnosti komunikací) a další osobní údaje (prostřednictvím žádosti o dobrovolné zpřístupnění) ([351]). Pokud jde o shromažďování komunikačních údajů (tj. obsahu komunikace nebo údajů potvrzujících komunikaci), platí omezení a záruky popsané v oddíle 3.3.1.1 včetně povinnosti získat soudem schválený příkaz. Pokud jde o žádosti o dobrovolné zpřístupnění jiných druhů osobních údajů osob podezřelých z terorismu, musí Národní zpravodajská služba splnit požadavky ústavy a zákona o ochraně osobních údajů týkající se nezbytnosti a proporcionality (viz 164. bod odůvodnění) ([352]). Správci, kteří obdrží takové žádosti, mohou vyhovět dobrovolně za podmínek stanovených v zákoně o ochraně osobních údajů (například v souladu se zásadou minimalizace údajů a s omezením dopadu na soukromí dané fyzické osoby) ([353]). V tomto případě musí také splnit požadavek na vyrozumění dotčené osoby vyplývající z oznámení č. 2021-5 (viz 166. bod odůvodnění).

([345]) U opatření omezujících komunikaci musí být tyto záznamy uchovávány po dobu tří let, viz čl. 9 odst. 3 zákona o ochraně důvěrnosti komunikací a čl. 17 odst. 2 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací. Pokud jde o shromažďování údajů potvrzujících komunikaci, musí zpravodajské služby uchovávat záznamy o podání žádosti o takové údaje, jakož i písemnou žádost samotnou a evidovat instituci, která ji využila (čl. 13 odst. 5 a čl. 13-4 odst. 3 zákona o ochraně důvěrnosti komunikací). Poskytovatelé telekomunikačních služeb musí uchovávat záznamy po dobu sedmi let a dvakrát ročně podávat zprávy o četnosti zpřístupnění údajů ministrovi pro vědu a IKT (čl. 9 odst. 3 zákona o ochraně důvěrnosti komunikací ve spojení s čl. 13 odst. 7 zákona o ochraně důvěrnosti komunikací a čl. 37 odst. 4 a článkem 39 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací).

([346]) Ustanovení čl. 18 odst. 3 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.

([347]) Ustanovení čl. 9-2 odst. 3 a čl. 13 odst. 4 zákona o ochraně důvěrnosti komunikací. V oznámení musí být uvedena 1) skutečnost, že byly shromážděny údaje, 2) výkonná agentura a 3) doba výkonu opatření.

([348]) Ustanovení čl. 9-2 odst. 4 zákona o ochraně důvěrnosti komunikací. V takovém případě musí být oznámení podáno do 30 dnů, jakmile pominou důvody odkladu, viz čl. 13-4 odst. 2 a čl. 9-2 odst. 6 zákona o ochraně důvěrnosti komunikací.

([349]) Tzn. o členech teroristické skupiny (podle definice Organizace spojených národů, viz čl. 2 odst. 2 zákona o boji proti terorismu); osobách, které propagují a šíří myšlenky nebo taktiku teroristické skupiny, získávají nebo vynakládají finanční prostředky na terorismus nebo se zapojují do jiných činností v rámci přípravy, konspirace, propagace nebo podněcování terorismu; nebo osobách, u nichž existují oprávněné důvody pro podezření, že takovou činnost prováděly (čl. 2 odst. 3 zákona o boji proti terorismu). „Terorismus“ je v čl. 2 odst. 1 zákona o boji proti terorismu definován jako jednání prováděné za účelem bránění výkonu pravomoci státu, místní správy nebo zahraniční vlády (včetně mezinárodních organizací) nebo s cílem přimět tyto subjekty k jednání, které není jejich zákonnou povinností, nebo zastrašit veřejnost. Takové jednání může například zahrnovat usmrcení, únos nebo braní rukojmí; únos/obsazení, zničení nebo poškození lodi nebo letadla; použití biochemických, výbušných nebo zápalných zbraní s úmyslem způsobit smrt, vážné zranění nebo škodu a zneužívání jaderných nebo radioaktivních materiálů.

([350]) Ustanovení čl. 9 odst. 1 a 3 zákona o boji proti terorismu.

([351]) Ačkoli zákon boji proti terorismu uvádí i možnost shromažďování údajů o vstupu do Korejské republiky a opuštění Korejské republiky na základě zákona o přistěhovalectví a celního zákona, tyto zákony v současné době takové oprávnění nestanoví (viz oddíl 3.2.2.1 přílohy II). V žádném případě by se zásadně nevztahovaly na údaje předávané na základě tohoto rozhodnutí, neboť by se obvykle týkaly údajů, které by byly shromažďovány přímo korejskými orgány (spíše než přístupu k údajům, které byly dříve předány z Unie korejským správcům). Kromě toho zákon o boji proti terorismu uvádí zákon o oznamování a používání určitých informací o finančních transakcích jakožto právní základ pro shromažďování údajů o finančních transakcích. Jak je však vysvětleno v poznámce pod čarou č. 200, druhy údajů, které by bylo možné získat na základě tohoto zákona, nespadají do oblasti působnosti tohoto rozhodnutí. A konečně zákon o boji proti terorismu také stanoví, že Národní zpravodajská služba může shromažďovat údaje o poloze prostřednictvím nezávazných žádostí, a v takovém případě by poskytovatelé údajů o poloze mohli takové údaje dobrovolně zpřístupnit za podmínek stanovených v zákoně o ochraně osobních údajů (viz 193. bod odůvodnění) a v zákoně o údajích o poloze. Jak je však rovněž vysvětleno v poznámce pod čarou č. 17, údaje o poloze nebudou na základě tohoto rozhodnutí předávány z Unie korejským správcům, ale budou generovány v Koreji.

([352]) Viz příloha II oddíl 3.2.2.2.

([353]) Viz čl. 58 odst. 4 zákona o ochraně osobních údajů, který vyžaduje, aby osobní údaje byly zpracovávány v minimálním rozsahu nezbytném k dosažení zamýšleného účelu, a čl. 3 odst. 6 zákona o ochraně osobních údajů, který stanoví, že osobní údaje musí být zpracovány způsobem, který minimalizuje možnost narušení soukromí dané fyzické osoby. Viz také článek 59 body 2 a 3 zákona o ochraně osobních údajů, podle nichž je správcům zakázáno zpřístupňovat osobní údaje třetím stranám bez oprávnění.

3.3.1.3 Žádosti o dobrovolné zpřístupnění údajů účastníků

(194) Na základě zákona o telekomunikačních službách mohou poskytovatelé telekomunikačních služeb dobrovolně zpřístupnit údaje účastníků (viz 163. bod odůvodnění) na žádost zpravodajské agentury, která hodlá tyto údaje shromáždit, aby zabránila ohrožení národní bezpečnosti ([354]). Pokud jde o takové žádosti ze strany Národní zpravodajské služby, platí stejná omezení (vyplývající z ústavy, zákona o ochraně osobních údajů a zákona o telekomunikačních službách) jako v oblasti prosazování trestního práva, jak je uvedeno ve 164. bodě odůvodnění ([355]). Poskytovatelé telekomunikačních služeb nejsou povinni vyhovět a mohou tak učinit pouze za podmínek stanovených v zákoně o ochraně osobních údajů (zejména v souladu se zásadou minimalizace údajů a omezením dopadu na soukromí fyzické osoby, viz také 193. bod odůvodnění). Použijí se tytéž požadavky na vedení záznamů a informování předmětné fyzické osoby jako v oblasti prosazování trestního práva (viz 165. a 166. bod odůvodnění).

3.3.2 *Další použití shromážděných informací*

(195) Zpracování osobních údajů shromažďovaných korejskými orgány pro účely národní bezpečnosti podléhá zásadám účelového omezení (čl. 3 odst. 1 a 2 zákona o ochraně osobních údajů), zákonnosti a korektnosti zpracování (čl. 3 odst. 1 zákona o ochraně osobních údajů), proporcionality/minimalizace údajů (čl. 3 odst. 1 a 6 a článek 58 zákona o ochraně osobních údajů), přesnosti (čl. 3 odst. 3 zákona o ochraně osobních údajů, transparentnosti (čl. 3 odst. 5 zákona o ochraně osobních údajů), zabezpečení (čl. 58 odst. 4 zákona o ochraně osobních údajů) a omezení uložení (čl. 58 odst. 4 zákona o ochraně osobních údajů) ([356]). K případnému zpřístupnění osobních údajů třetím stranám (včetně třetích zemí) může dojít pouze v souladu s těmito zásadami (zejména zásadou účelového omezení a minimalizace údajů) a po posouzení souladu se zásadami nezbytnosti a proporcionality (čl. 37 odst. 2 ústavy) a s přihlédnutím k dopadu na práva dotčených osob (čl. 3 odst. 6 zákona o ochraně osobních údajů).

(196) Pokud jde o obsah komunikace a údaje potvrzující komunikaci, zákon o ochraně důvěrnosti komunikací dále omezuje použití těchto údajů na soudní řízení, v němž se na tyto údaje strana, které se komunikace týká, odvolává v rámci nároku na náhradu škody, nebo povolená použití podle jiných právních předpisů ([357]).

3.3.3 *Dozor*

(197) Dozor nad činností korejských vnitrostátních bezpečnostních orgánů zajišťují různé subjekty ([358]).

(198) Zaprvé zákon o boji proti terorismu stanoví zvláštní mechanismy dozoru nad protiteroristickými činnostmi včetně shromažďování údajů o osobách podezřelých z terorismu. Konkrétně na úrovni výkonné moci protiteroristické činnosti dozoruje Komise pro boj proti terorismu ([359]), které je ředitel Národní zpravodajské služby povinen podávat zprávy o vyšetřování a pátrání po osobách podezřelých z terorismu ve spojitosti se shromažďováním údajů nebo materiálů nezbytných pro protiteroristickou činnost ([360]). Vedle toho pověřenec pro ochranu lidských práv konkrétně dohlíží na soulad činností v oblasti boje proti terorismu se základními právy ([361]). Pověřence pro ochranu lidských práv jmenuje předseda Komise pro boj proti terorismu z řad osob, které splňují konkrétní požadavky uvedené v prováděcí vyhlášce k zákonu o boji proti terorismu ([362]), a to na dvouleté funkční období (s možností prodloužení), přičemž pověřenec může být z funkce odvolán pouze ze specifických, omezených a oprávněných důvodů ([363]). V rámci výkonu své dozorové funkce může pověřenec pro ochranu lidských

([354]) Ustanovení čl. 83 odst. 3 zákona o telekomunikačních službách.
([355]) Viz také příloha II oddíl 3.2.3.
([356]) Viz příloha II oddíl 1.2.
([357]) Ustanovení čl. 5 odst. 1 a 2 a článků 12 a 13-5 zákona o ochraně důvěrnosti komunikací.
([358]) Viz příloha II oddíl 3.3.
([359]) Ustanovení čl. 5 odst. 3 zákona o boji proti terorismu. Komisi předsedá předseda vlády a tvoří ji několik ministrů a vedoucích představitelů vládních agentur, např. ministři zahraničních věcí, spravedlnosti, národní obrany a vnitra a bezpečnosti, ředitel Národní zpravodajské služby a generální komisař Národní policejní agentury (čl. 3 odst. 1 prováděcí vyhlášky k zákonu o boji proti terorismu).
([360]) Ustanovení čl. 9 odst. 4 zákona o boji proti terorismu.
([361]) Článek 7 zákona o boji proti terorismu.
([362]) Tj. kdokoli s kvalifikací advokáta a nejméně desetiletou praxí nebo osoba s odbornou znalostí v oblasti lidských práv, která nejméně deset let pracuje nebo pracovala (alespoň) jako vysokoškolský docent nebo jako vyšší státní úředník ve státních agenturách nebo v orgánech místní správy, nebo osoba s nejméně desetiletou pracovní praxí v oblasti lidských práv, např. v nevládní organizaci (čl. 7 odst. 1 prováděcí vyhlášky k zákonu o boji proti terorismu).
([363]) Například je-li obžalován v trestní věci související s jeho povinnostmi, při vyzrazení důvěrných informací nebo z důvodu dlouhodobé duševní či fyzické nezpůsobilosti (čl. 7 odst. 3 prováděcí vyhlášky k zákonu o boji proti terorismu).

práv vydávat obecná doporučení k zlepšení ochrany lidských práv ([364]) a konkrétní doporučení ohledně nápravných opatření v případě, že je zjištěno porušení lidských práv ([365]). Orgány veřejné správy jsou povinny pověřence pro ochranu lidských práv informovat o opatřeních přijatých v návaznosti na jeho doporučení ([366]).

(199) Zadruhé Komise pro ochranu osobních údajů zajišťuje dozor nad tím, jak orgány v oblasti národní bezpečnosti dodržují pravidla ochrany osobních údajů, což zahrnuje použitelná ustanovení zákona o ochraně osobních údajů (viz 149. bod odůvodnění) i omezení a záruky týkající se shromažďování osobních údajů podle jiných právních předpisů (zákona o ochraně důvěrnosti sdělen, zákona o boji proti terorismu a zákona o telekomunikačních službách, viz také 171. bod odůvodnění) ([367]). Při výkonu této dozorové úlohy může Komise pro ochranu osobních údajů využít všech svých vyšetřovacích a nápravných pravomocí, podrobně popsaných v oddíle 2.4.2.

(200) Zatřetí činnosti orgánů v oblasti národní bezpečnosti podléhají nezávislému dozoru ze strany Národní komise pro lidská práva v souladu s postupy popsanými ve 172. bodě odůvodnění ([368]).

(201) Začtvrté se na vnitrostátní bezpečnostní orgány vztahuje dozorová funkce Rady pro audit a inspekce, přestože Národní zpravodajská služba může za výjimečných okolností odmítnout poskytnout určité údaje nebo materiály, pokud představují státní tajemství a pokud by zveřejnění mělo závažný dopad na národní bezpečnost ([369]).

(202) A konečně parlamentní dozor nad činností Národní zpravodajské služby vykonává Národní shromáždění (prostřednictvím specializovaného zpravodajského výboru) ([370]). Zákon o ochraně důvěrnosti komunikací stanoví zvláštní dozorovou úlohu Národního shromáždění s ohledem na používání opatření omezujících komunikaci pro účely národní bezpečnosti ([371]). Národní shromáždění může zejména provádět kontroly odposlechového zařízení na místě a může vyžadovat, aby Národní zpravodajská služba i poskytovatelé telekomunikačních služeb, kteří zpřístupnili obsah komunikace, o tom předložili zprávu. Národní shromáždění může také vykonávat své obecné dozorové funkce (v souladu s postupy popsanými ve 174. bodě odůvodnění). Zákon o Národní zpravodajské službě vyžaduje, aby ředitel Národní zpravodajské služby bezodkladně odpověděl, pokud si zpravodajský výbor vyžádá zprávu o konkrétní záležitosti ([372]), přičemž pro určité zvláště citlivé údaje platí zvláštní pravidla. Konkrétně ředitel Národní zpravodajské služby může odmítnout odpovědět nebo vypovídat před zpravodajským výborem jen za výjimečných okolností, tj. pokud jsou předmětem žádosti státní tajemství týkající se vojenských a diplomatických záležitostí nebo záležitostí souvisejících se Severní Koreou, u nichž by zveřejnění mohlo mít vážný dopad na „národní osud" země ([373]). V tomto případě může zpravodajský výbor požádat o vysvětlení předsedu vlády, a pokud toto vysvětlení není podáno do sedmi dnů, odpověď nebo výpověď již nelze odmítnout.

3.3.4 *Opravné prostředky*

(203) I v oblasti národní bezpečnosti nabízí korejský systém různé (soudní) cesty k dosažení nápravy, včetně náhrady škody. Tyto mechanismy poskytují subjektům údajů účinné prostředky správní a soudní ochrany, které jim umožňují zejména výkon jejich práv včetně práva na přístup k jejich osobním údajům nebo na dosažení opravy či výmazu těchto údajů.

(204) Zaprvé mohou podle čl. 3 odst. 5 a čl. 4 odst. 1, 3 a 4 zákona o ochraně osobních údajů fyzické osoby uplatňovat vůči vnitrostátním bezpečnostním orgánům svá práva na přístup, opravu, výmaz a pozastavení zpracování. Oddíl 6 oznámení č. 2021-5 (příloha I tohoto rozhodnutí) dále objasňuje, jak se tato práva uplatňují v souvislosti

([364]) Ustanovení čl. 8 odst. 1 prováděcí vyhlášky k zákonu o boji proti terorismu.

([365]) Ustanovení čl. 9 odst. 1 prováděcí vyhlášky k zákonu o boji proti terorismu. Pověřenec pro ochranu lidských práv rozhoduje o přijetí doporučení autonomně, je však povinen oznámit tato doporučení předsedovi Komise pro boj proti terorismu.

([366]) Ustanovení čl. 9 odst. 2 prováděcí vyhlášky k zákonu o boji proti terorismu. Pokud by doporučení pověřence pro ochranu lidských práv nebylo provedeno, byla by záležitost podle oficiálního prohlášení korejské vlády postoupena Komisi pro boj proti terorismu, včetně předsedy vlády, dosud se však nevyskytly případy, kdy by doporučení pověřence pro ochranu lidských práv nebyla provedena (viz oddíl 3.3.1 přílohy II).

([367]) Příloha II oddíl 3.3.4.

([368]) Konkrétně pokud jde o Národní zpravodajskou službu, Národní komise pro lidská práva v minulosti prováděla vyšetřování z moci úřední a vyřizovala řadu jednotlivých stížností. Viz např. výroční zpráva Národní komise pro lidská práva za rok 2018, s. 128 (k dispozici na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) a výroční zpráva Národní komise pro lidská práva za rok 2019, s. 70 (k dispozici na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([369]) Ustanovení čl. 13 odst. 1 zákona o Národní zpravodajské službě.

([370]) Článek 36 a čl. 37 odst. 1 bod 15 zákona o Národním shromáždění.

([371]) Článek 15 zákona o ochraně důvěrnosti komunikací.

([372]) Ustanovení čl. 15 odst. 2 zákona o Národní zpravodajské službě.

([373]) Ustanovení čl. 17 odst. 2 zákona o Národní zpravodajské službě. „Státní tajemství" jsou definována jako (utajované) skutečnosti, věci nebo znalosti, které nesmějí být zpřístupněny jiné zemi nebo organizaci, aby se předešlo závažnému narušení národní bezpečnosti, a k nimž je povolen pouze omezený přístup. Viz čl. 13 odst. 4 zákona o Národní zpravodajské službě.

se zpracováním údajů pro účely národní bezpečnosti. Orgán v oblasti národní bezpečnosti může zejména omezit nebo odepřít výkon práva, pokud a dokud je to nezbytné a přiměřené k ochraně důležitého cíle veřejného zájmu (například v takovém rozsahu a po takovou dobu, kdy by udělení práva ohrozilo probíhající vyšetřování nebo národní bezpečnost), nebo pokud udělení práva může způsobit újmu na životě nebo zdraví třetí strany. Uplatnění takovéhoto omezení proto vyžaduje vyvážení práv a zájmů jednotlivce vůči příslušnému veřejnému zájmu a nesmí se v žádném případě dotknout podstaty práva (čl. 37 odst. 2 ústavy). Pokud je žádost zamítnuta nebo omezena, musí být fyzické osobě neprodleně oznámeny příslušné důvody.

(205) Zadruhé mají fyzické osoby právo využít různé nápravné mechanismy podle zákona o ochraně osobních údajů, pokud jejich údaje zpracoval orgán v oblasti národní bezpečnosti v rozporu se zákonem o ochraně osobních údajů nebo v rozporu s omezeními a zárukami podle jiných právních předpisů upravujících shromažďování osobních údajů (zejména zákona o ochraně důvěrnosti komunikací, viz 171. bod odůvodnění) ([374]). Toto právo lze uplatnit podáním stížností u Komise pro ochranu osobních údajů prostřednictvím kontaktního centra pro ochranu soukromí, které provozuje Korejská agentura pro internet a bezpečnost ([375])). Aby se umožnil snadnější přístup k opravným prostředkům vůči korejským vnitrostátním bezpečnostním orgánům, fyzické osoby z EU mohou dále podat stížnost u Komise pro ochranu osobních údajů prostřednictvím svého vnitrostátního orgánu pro ochranu údajů ([376]). V takovém případě Komise pro ochranu osobních údajů prostřednictvím vnitrostátního úřadu pro ochranu osobních údajů fyzickou osobu informuje, jakmile je vyšetřování ukončeno (případně včetně informací o uložených nápravných opatřeních). Podle zákona o správním soudním řízení mohou také fyzické osoby podat opravný prostředek proti rozhodnutím nebo nečinnosti / napadnout rozhodnutí nebo nečinnost Komise pro ochranu osobních údajů (viz 132. bod odůvodnění).

(206) Zatřetí mohou fyzické osoby podat pověřenci pro ochranu lidských práv stížnost na porušení jejich práva na soukromí / ochranu údajů v souvislosti s protiteroristickými činnostmi (tj. podle zákona o boji proti terorismu) ([377]) a pověřenec může doporučit nápravná opatření. Vzhledem k tomu, že u pověřence pro ochranu lidských práv neexistují žádné požadavky na přípustnost, bude stížnost vyřízena i v případě, že dotčená osoba nemůže prokázat, že skutečně utrpěla újmu (například kvůli údajně nezákonnému shromažďování jejích údajů orgánem v oblasti národní bezpečnosti) ([378]). Příslušný orgán musí pověřence pro ochranu lidských práv informovat o všech opatřeních přijatých k provedení jeho doporučení.

(207) Začtvrté mohou fyzické osoby podat Národní komisi pro lidská práva stížnost týkající se shromažďování jejich údajů vnitrostátními bezpečnostními orgány a dosáhnout nápravy v souladu s postupem popsaným ve 178. bodě odůvodnění ([379]).

(208) A konečně jsou k dispozici různé soudní opravné prostředky ([380]), které fyzickým osobám umožňují dovolávat se dosažení nápravy omezení a záruk popsaných v oddíle 3.3.1. Fyzické osoby mohou zejména napadnout zákonnost postupu vnitrostátních bezpečnostních orgánů na základě zákona o správním soudním řízení (postupem popsaným ve 181. bodě odůvodnění) nebo zákona o Ústavním soudu (viz 182. bod odůvodnění). Kromě toho mohou získat náhradu škody na základě zákona o náhradě škody státem (jak je podrobněji popsáno ve 183. bodě odůvodnění).

4. ZÁVĚR

(209) Komise má za to, že prostřednictvím zákona o ochraně osobních informací, zvláštních pravidel použitelných na určitá odvětví (analyzovaných v oddíle 2) a dalších záruk stanovených v oznámení č. 2021-5 (příloha I) Korejská republika zajišťuje úroveň ochrany osobních údajů předávaných z Evropské unie, která je v zásadě rovnocenná úrovni ochrany zaručené nařízením (EU) 2016/679.

(210) Kromě toho má Komise za to, že jako celek dozorové mechanismy a způsoby ochrany v korejských právních předpisech umožňují, aby porušení zabezpečení osobních údajů ze strany správců v Koreji byla identifikována a v praxi řešena, a subjektu údajů nabízí právní prostředky pro získání přístupu k jeho osobním údajům a případně opravu nebo výmaz takovýchto údajů.

([374]) Ustanovení čl. 58 odst. 4 a čl. 4 odst. 5 zákona o ochraně osobních údajů. Viz příloha II bod 3.4.2.
([375]) Článek 62 a čl. 63 odst. 2 zákona o ochraně osobních údajů.
([376]) Oznámení č. 2021-5 (příloha I oddíl 6).
([377]) Ustanovení čl. 8 odst. 1 bodu 2 prováděcí vyhlášky k zákonu o boji proti terorismu.
([378]) Viz příloha II oddíl 3.4.1.
([379]) Národní komise pro lidská práva například pravidelně přijímá stížnosti na Národní zpravodajskou službu, viz údaje z výroční zprávy Národní komise pro lidská práva za rok 2019 o počtu stížností obdržených v letech 2015 až 2019, s. 70 (k dispozici na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Viz příloha II oddíl 3.4.4.

(211) V neposlední řadě na základě dostupných informací o korejském právním řádu, včetně prohlášení, ujištění a závazků korejské vlády obsažených v příloze II, má Komise za to, že jakýkoli zásah do základních práv fyzických osob, jejichž osobní údaje se předávají z Evropské unie do Korejské republiky, ze strany korejských orgánů veřejné správy pro účely veřejného zájmu – zejména pro účely prosazování trestního práva a národní bezpečnosti – bude omezen na rozsah nezbytně nutný pro dosažení daného oprávněného cíle a že existuje účinná právní ochrana před takovým zásahem.

(212) S ohledem na zjištění tohoto rozhodnutí by proto mělo být rozhodnuto, že Korejská republika zajišťuje odpovídající úroveň ochrany ve smyslu článku 45 nařízení (EU) 2016/679 vykládaného z hlediska Listiny základních práv Evropské unie, pokud jde o osobní údaje předávané z Evropské unie do Korejské republiky správcům osobních údajů v Korejské republice, na které se použije zákon o ochraně osobních údajů, s výjimkou náboženských organizací, pokud zpracovávají osobní údaje pro svou misijní činnost, politických stran, pokud zpracovávají osobní údaje v souvislosti s nominací kandidátů, a správců, kteří podléhají dozoru Komise pro finanční služby při zpracování osobních úvěrových informací podle zákona o úvěrových informacích, pokud zpracovávají takové informace.

5. ÚČINKY TOHOTO ROZHODNUTÍ A ČINNOST ÚŘADŮ PRO OCHRANU ÚDAJŮ

(213) Členské státy a jejich orgány musí přijmout opatření nezbytná k dosažení souladu s akty orgánů Unie, neboť jim v zásadě svědčí presumpce legality, a tudíž zakládají právní účinky tak dlouho, dokud nejsou vzaty zpět, zrušeny v rámci žaloby na neplatnost nebo prohlášeny za neplatné v návaznosti na žádost o rozhodnutí o předběžné otázce nebo na námitku protiprávnosti.

(214) V důsledku toho je rozhodnutí Komise o odpovídající ochraně podle čl. 45 odst. 3 nařízení (EU) 2016/679 závazné pro všechny orgány členských států, kterým je určeno, a to i pro nezávislé dozorové úřady. Zejména může docházet k předáním od správce nebo zpracovatele v Evropské unii správcům v Korejské republice, aniž by bylo nutné získat další povolení.

(215) Je třeba připomenout, že podle čl. 58 odst. 5 nařízení (EU) 2016/679 a podle vysvětlení Soudního dvora v rozsudku ve věci Schrems ([381]), jestliže vnitrostátní orgán pro ochranu údajů zpochybňuje, a to i na základě stížnosti, slučitelnost rozhodnutí Komise o odpovídající ochraně se základními právy fyzické osoby na soukromí a ochranu údajů, musí mu vnitrostátní právo poskytnout procesní prostředek, který mu umožní uplatnit tyto výtky před vnitrostátním soudem, který může být povinen předložit Soudnímu dvoru žádost o rozhodnutí o předběžné otázce ([382]).

6. MONITOROVÁNÍ A PŘEZKUM TOHOTO ROZHODNUTÍ

(216) Podle judikatury Soudního dvora ([383]), a jak je uznáno v článku čl. 45 odst. 4 nařízení (EU) 2016/679, by Komise po přijetí rozhodnutí o odpovídající ochraně měla neustále sledovat příslušný vývoj v dotyčné třetí zemi, aby mohla posoudit, zda tato třetí země stále zajišťuje v zásadě rovnocennou úroveň ochrany. Takové ověřování je každopádně závazné tehdy, když Komise obdrží informace vyvolávající v tomto ohledu určité odůvodněné pochybnosti.

(217) Komise by tedy měla průběžně sledovat situaci v Korejské republice, pokud jde o právní rámec a skutečnou praxi zpracování osobních údajů, jak jsou posouzeny v tomto rozhodnutí, včetně toho, zda korejské orgány dodržují prohlášení, ujištění a závazky obsažené v příloze II. K usnadnění tohoto procesu se korejské orgány vyzývají, aby Komisi urychleně informovaly o podstatném vývoji relevantním pro toto rozhodnutí, pokud jde o zpracování osobních údajů podnikatelskými subjekty a orgány veřejné správy i o omezení a záruky použitelné pro přístup k osobním údajům ze strany orgánů veřejné správy.

([381]) Rozsudek ve věci Schrems, bod 65.

([382]) Rozsudek ve věci Schrems, bod 65: „V tomto ohledu přísluší vnitrostátnímu normotvůrci, aby stanovil procesní prostředky, které by dotyčnému vnitrostátnímu orgánu dozoru umožnily uplatnit výtky, jež považuje za opodstatněné, před vnitrostátními soudy, aby tyto soudy v případě, že sdílejí pochybnosti vyjádřené tímto orgánem ohledně platnosti rozhodnutí Komise, předložily žádost o rozhodnutí o předběžné otázce za účelem přezkumu platnosti tohoto rozhodnutí."

([383]) Rozsudek ve věci Schrems, bod 76.

(218) Aby Komise navíc mohla účinně plnit svou kontrolní funkci, měly by ji členské státy informovat o veškerých relevantních krocích vnitrostátních úřadů pro ochranu údajů, zejména v souvislosti s dotazy nebo stížnostmi subjektů údajů z EU týkajícími se předávání osobních údajů z Evropské unie správcům údajů v Korejské republice. Komise by rovněž měla být informována o jakýchkoli známkách toho, že kroky korejských orgánů veřejné správy odpovědných za prevenci, vyšetřování, odhalování nebo stíhání trestných činů nebo za národní bezpečnost, včetně jakýchkoli dozorových subjektů, nezajišťují požadovanou úroveň ochrany.

(219) Podle čl. 45 odst. 3 nařízení (EU) 2016/679 ([384]) a s ohledem na skutečnost, že úroveň ochrany poskytovaná korejským právním řádem se může změnit, měla by Komise po přijetí tohoto rozhodnutí pravidelně ověřovat, zda zjištění týkající se odpovídající úrovně ochrany zajištěné Korejskou republikou jsou nadále skutkově i právně podložená.

(220) Za tímto účelem by toto rozhodnutí mělo být předmětem prvního přezkumu do tří let po jeho vstupu v platnost. Po tomto prvním přezkumu a v závislosti na jeho výsledku Komise v úzké konzultaci s výborem zřízeným podle čl. 93 odst. 1 nařízení (EU) 2016/679 rozhodne, zda by měl být tříletý cyklus zachován. V každém případě by se následné přezkumy měly provádět alespoň každé čtyři roky ([385]). Přezkum by měl zahrnovat všechny aspekty fungování tohoto rozhodnutí, a zejména použití dalších záruk obsažených v příloze I tohoto rozhodnutí, se zvláštní pozorností věnovanou ochraně poskytované v případě dalšího předávání; vývoj relevantní judikatury; pravidla týkající se zpracování pseudonymizovaných údajů pro účely statistiky, vědeckého výzkumu a archivace ve veřejném zájmu, jakož i použití výjimek podle čl. 28 odst. 7 zákona o ochraně osobních údajů; účinnost výkonu individuálních práv, včetně doby před nedávnou reformou zákona o ochraně osobních údajů, a použití výjimek z těchto práv; použití dílčích výjimek podle zákona o ochraně osobních údajů; jakož i omezení a záruky, pokud jde o přístup vlády (stanovené v příloze II tohoto rozhodnutí), včetně spolupráce Komise pro ochranu osobních údajů s úřady pro ochranu údajů v EU ve věci stížností fyzických osob. Měl by rovněž zahrnovat účinnost dozoru a prosazování práva, pokud jde o zákon o ochraně osobních údajů a oblast prosazování trestního práva a národní bezpečnosti (zejména ze strany Komise pro ochranu osobních údajů a Národní komise pro lidská práva).

(221) K provedení přezkumu by se Komise měla setkat s Komisí pro ochranu osobních údajů, v příslušných případech doprovázenou dalšími korejskými orgány odpovědnými za přístup vlády, včetně příslušných dozorových subjektů. Účast na této schůzce by měla být otevřena zástupcům členů Evropského sboru pro ochranu osobních údajů. V rámci přezkumu by Komise měla požadovat, aby Komise pro ochranu osobních údajů poskytla souhrnné informace o všech aspektech relevantních pro zjištění o odpovídající úrovni ochrany, včetně omezení a záruk týkajících se přístupu ze strany vlády ([386]). Komise by měla rovněž požadovat vysvětlení jakýchkoli obdržených informací relevantních pro toto rozhodnutí, včetně veřejných zpráv korejských orgánů nebo jiných zúčastněných stran v Koreji, Evropského sboru pro ochranu osobních údajů, jednotlivých úřadů pro ochranu osobních údajů, skupin občanské společnosti, tiskových zpráv nebo jakéhokoli jiného dostupného zdroje informací.

(222) Na základě přezkumu by Komise měla připravit veřejně přístupnou zprávu, kterou předloží Evropskému parlamentu a Radě.

7. POZASTAVENÍ POUŽITELNOSTI, ZRUŠENÍ NEBO ZMĚNA TOHOTO ROZHODNUTÍ

(223) Pokud z dostupných informací, zejména z informací vyplývajících ze sledování tohoto rozhodnutí nebo poskytnutých orgány Koreje nebo členských států, vyplyne, že úroveň ochrany poskytované Korejskou republikou již nemusí být odpovídající, měla by Komise urychleně informovat příslušné korejské orgány a požadovat, aby byla ve stanovené a přiměřené lhůtě přijata vhodná opatření.

(224) Pokud po uplynutí stanovené lhůty příslušné korejské orgány tato opatření nepřijmou nebo jiným způsobem uspokojivě neprokážou, že toto rozhodnutí je nadále založeno na odpovídající úrovni ochrany, zahájí Komise postup podle čl. 93 odst. 2 nařízení (EU) 2016/679 s cílem částečně nebo úplně zrušit toho rozhodnutí nebo pozastavit jeho platnost.

(225) Alternativně Komise tento postup zahájí s cílem změnit toto rozhodnutí, zejména tím, že se na předávání údajů budou vztahovat další podmínky nebo že se omezí oblasti působnosti zjištění o odpovídající úrovni ochrany jen na předávání údajů, u nichž je odpovídající úroveň ochrany nadále zaručena.

([384]) Podle čl. 45 odst. 3 nařízení (EU) 2016/679 „[u]vedený prováděcí akt stanoví mechanismus pro pravidelný přezkum […], který zohlední veškerý relevantní vývoj v dotčené třetí zemi nebo mezinárodní organizaci".

([385]) V čl. 45 odst. 3 nařízení (EU) 2016/679 se stanoví, že pravidelný přezkum se musí provádět „nejméně každé čtyři roky". Viz také Evropský sbor pro ochranu osobních údajů, Referenční rámec pro odpovídající ochranu, WP 254 rev. 01.

([386]) Viz příloha II tohoto rozhodnutí.

(226) Zejména by Komise měla zahájit postup k pozastavení platnosti nebo zrušení tohoto rozhodnutí, pokud existují známky toho, že další záruky obsažené v příloze I nejsou podnikatelskými subjekty přijímajícími osobní údaje podle tohoto rozhodnutí dodržovány a/nebo účinně vymáhány nebo že korejské orgány nedodržují prohlášení, ujištění a závazky obsažené v příloze II tohoto rozhodnutí.

(227) Komise by rovněž měla zvážit zahájení postupu vedoucího ke změně, pozastavení platnosti nebo zrušení tohoto rozhodnutí, pokud v souvislosti s přezkumem nebo jinak neposkytnou příslušné korejské orgány informace nebo objasnění nezbytná k posouzení úrovně ochrany poskytované osobním údajům předávaným z Evropské unie do Korejské republiky nebo dodržování tohoto rozhodnutí. V tomto směru by Komise měla vzít v potaz míru, do jaké lze relevantní informace získat z jiných zdrojů.

(228) V závažných, naléhavých a řádně odůvodněných případech Komise využije možnost postupem podle čl. 93 odst. 3 nařízení (EU) 2016/679 přijmout okamžitě použitelné prováděcí akty, kterými se rozhodnutí zruší, změní nebo se dočasně pozastaví jeho platnost.

8. **ZÁVĚREČNÉ ÚVAHY**

(229) Evropský sbor pro ochranu osobních údajů zveřejnil své stanovisko ([387]), které bylo při přípravě tohoto rozhodnutí zohledněno.

(230) Opatření stanovená tímto rozhodnutím jsou v souladu se stanoviskem výboru zřízeného podle čl. 93 odst. 1 nařízení (EU) 2016/679,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

1. Pro účely článku 45 nařízení (EU) 2016/679 Korejská republika zajišťuje odpovídající úroveň ochrany osobních údajů předávaných z Evropské unie subjektům v Korejské republice podle zákona o ochraně osobních údajů, doplněného o další záruky stanovené v příloze I, společně s oficiálními prohlášeními, ujištěními a závazky obsaženými v příloze II.

2. Toto rozhodnutí se nevztahuje na osobní údaje předávané příjemcům, kteří spadají do jedné z níže uvedených kategorií, v rozsahu, ve kterém účely zpracování osobních údajů zcela nebo částečně odpovídají jednomu ze zde uvedených účelů, konkrétně:

a) náboženským organizacím, pokud zpracovávají osobní údaje pro svou misijní činnost;

b) politickým stranám, pokud zpracovávají osobní údaje v souvislosti s nominací kandidátů;

c) subjektům, které podléhají dozoru Komise pro finanční služby při zpracování osobních úvěrových informací podle zákona o úvěrových informacích, pokud takové informace zpracovávají.

Článek 2

Pokud příslušné orgány v členských státech za účelem ochrany fyzických osob s ohledem na zpracování jejich osobních údajů uplatní pravomoc podle článku 58 nařízení (EU) 2016/679, pokud jde o předávání údajů spadající do oblasti působnosti stanovené v článku 1 tohoto rozhodnutí, oznámí dotyčný členský stát tuto skutečnost bezodkladně Komisi.

Článek 3

1. Komise neustále sleduje uplatňování právního rámce, na němž je založeno toto rozhodnutí, včetně podmínek, za kterých dochází k dalšímu předávání, výkonu individuálních práv a přístupu korejských orgánů veřejné správy k údajům předaným na základě tohoto rozhodnutí, s cílem posoudit, zda Korejská republika i nadále zajišťuje odpovídající úroveň ochrany ve smyslu článku 1.

([387]) Stanovisko č. 32/2021 k návrhu prováděcího rozhodnutí podle nařízení (EU) 2016/679 o odpovídající ochraně osobních údajů poskytované Korejskou republikou, který předložila Evropská komise, k dispozici na této adrese: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. Členské státy a Komise se vzájemně informují o případech, kdy Komise pro ochranu osobních informací nebo jakýkoli jiný příslušný korejský orgán nezajišťuje soulad s právním rámcem, na němž je toto rozhodnutí založeno.

3. Členské státy a Komise se vzájemně informují o jakýchkoli známkách toho, že zásahy korejských orgánů veřejné správy do práva fyzických osob na ochranu jejich osobních údajů přesahují rámec toho, co je nezbytně nutné, nebo že proti takovým zásahům není účinné právní ochrany.

4. Po třech letech ode dne oznámení tohoto rozhodnutí členským státům a poté nejméně každé čtyři roky Komise vyhodnotí zjištění uvedené v čl. 1 odst. 1 na základě veškerých dostupných informací, včetně informací získaných v rámci přezkumu provedeného společně s příslušnými korejskými orgány.

5. Pokud má Komise informace o tom, že odpovídající úroveň ochrany již není zajištěna, informuje příslušné korejské orgány. Případně může rozhodnout o pozastavení použitelnosti, změně nebo zrušení tohoto rozhodnutí nebo o omezení jeho působnosti podle čl. 45 odst. 5 nařízení (EU) 2016/679, zejména zjistí-li známky toho, že:

a) správci v Koreji, kteří přijali osobní údaje z Evropské unie podle tohoto rozhodnutí, nedodržují další záruky obsažené v příloze I nebo že v tomto ohledu jsou dozor a prosazování práva nedostačující;

b) korejské orgány veřejné správy nedodržují prohlášení, ujištění a závazky obsažené v příloze II, včetně těch, které se týkají podmínek a omezení pro shromažďování osobních údajů předávaných podle tohoto rozhodnutí a přístupu k nim ze strany korejských orgánů veřejné správy pro účely prosazování trestního práva nebo národní bezpečnosti.

Komise může taková opatření přijmout také v případě, kdy nedostatečná spolupráce korejské vlády brání Komisi v určení toho, zda Korejská republika i nadále zajišťuje odpovídající úroveň ochrany.

Článek 4

Toto rozhodnutí je určeno členským státům.

V Bruselu dne 17. prosince 2021.

Za Komisi
Didier REYNDERS
člen Komise

PŘÍLOHA I

DOPLŇKOVÁ PRAVIDLA K VÝKLADU A POUŽITÍ ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ PŘEDÁVANÝCH KOREJI

Obsah

I. Úvod

Korea a Evropská unie (dále jen „EU“) vedly jednání o odpovídající ochraně, na jejichž základě Evropská unie došla k závěru, že Korea zaručuje odpovídající úroveň ochrany osobních údajů podle článku 45 obecného nařízení o ochraně osobních údajů.

V této souvislosti přijala Komise pro ochranu osobních údajů toto oznámení podle článku 5 (Povinnosti státu atd.) a článku 14 (Mezinárodní spolupráce) ([1]) zákona o ochraně osobních údajů s cílem vyjasnit výklad, uplatňování a prosazování některých ustanovení zákona, a to i pokud jde o zpracování osobních údajů předávaných do Koreje na základě rozhodnutí EU o odpovídající ochraně.

Vzhledem k tomu, že toto oznámení má status správního předpisu, který příslušná správní agentura zavádí a vyhlašuje za účelem vyjasnění standardů pro výklad, použití a vymáhání zákona o ochraně osobních údajů v rámci právního systému Koreje, je pro správce osobních údajů právně závazné v tom smyslu, že jakékoli porušení tohoto oznámení může být považováno za porušení příslušných ustanovení zákona o ochraně osobních údajů. Kromě toho, pokud v důsledku porušení tohoto oznámení dojde k porušení osobních práv a zájmů, jsou příslušné osoby oprávněny domáhat se nápravy u Komise pro ochranu osobních údajů nebo u soudu.

Pokud tedy správce osobních údajů, který zpracovává osobní údaje předané do Koreje podle rozhodnutí EU o odpovídající ochraně, nepřijme opatření v souladu s tímto oznámením, bude se mít za to, „že existuje závažný důvod se domnívat, že došlo k porušení předpisů v oblasti osobních údajů, a nečinnost pravděpodobně způsobí obtížně napravitelnou škodu“ podle odstavců 1 a 2 článku 64 zákona. V takových případech může Komise pro ochranu osobních

([1]) Článek 14 zákona o ochraně osobních údajů vymezuje pravomoc korejské vlády stanovit koncepce za účelem zlepšení úrovně ochrany osobních údajů v mezinárodním prostředí a předcházet porušování práv subjektů údajů v důsledku přeshraničního předávání osobních údajů.

údajů nebo související ústřední správní agentura příslušnému správci osobních údajů na základě pravomoci dané tímto ustanovením nařídit, aby přijal nápravná a další opatření, a podle konkrétního porušení zákona lze také uložit odpovídající trest (sankce, správní pokuty atd.).

II. **Definice pojmů**

Definice pojmů použitých v tomto ustanovení:

(i) zákon: zákon o ochraně osobních údajů (zákon č. 16930 ve znění ze dne 4. února 2020 s účinností ke dni 5. srpna 2020);

(ii) prezidentská vyhláška: prováděcí vyhláška k zákonu o ochraně osobních údajů (prezidentská vyhláška č. 30509, 3. března 2020, kterou se mění další zákony);

(iii) subjekt údajů: fyzická osoba, která je identifikovatelná na základě údajů zpracovávaných podle těchto pravidel, jež se stává subjektem těchto údajů;

(iv) správce osobních údajů: veřejná instituce, právnická osoba, organizace, fyzická osoba atd., která v rámci své činnosti přímo nebo nepřímo zpracovává osobní údaje;

(v) EU: EU (ke konci února 2020 tvoří EU 27 členských zemí ([2]), a to Belgie, Německo, Francie, Itálie, Lucembursko, Nizozemsko, Dánsko, Irsko, Řecko, Portugalsko, Španělsko, Rakousko, Finsko, Švédsko, Kypr, Česká republika, Estonsko, Maďarsko, Lotyšsko, Litva, Malta, Polsko, Slovensko, Slovinsko, Rumunsko, Bulharsko a Chorvatsko), jakož i země přidružené k EU prostřednictvím Dohody o EHP (Island, Lichtenštejnsko, Norsko);

(vi) GDPR: obecný právní předpis Evropské unie o ochraně osobních údajů, obecné nařízení o ochraně osobních údajů (nařízení (EU) 2016/679);

(vii) rozhodnutí o odpovídající úrovni ochrany: podle čl. 45 odst. 3 nařízení GDPR Evropská komise rozhodla, že určitá třetí země, určité území třetí země, jedna či více oblastí nebo mezinárodní organizace zajišťují odpovídající úroveň ochrany osobních údajů.

III. **Doplňková pravidla**

1. **Omezení používání a poskytování osobních údajů za jiným než určeným účelem (články 3, 15 a 18 zákona)**

<Zákon o ochraně osobních údajů

(zákon č. 16930 ve znění částečně pozměněném dne 4. února 2020)>

Článek 3 (Zásady ochrany osobních údajů) 1) Správce osobních údajů výslovně stanoví účely, pro které jsou osobní údaje zpracovávány, a shromažďuje osobní údaje zákonným a korektním způsobem v minimálním rozsahu nezbytném pro tyto účely.

2) Správce osobních údajů zpracovává osobní údaje vhodným způsobem, který je nezbytný pro účely, pro které jsou osobní údaje zpracovávány, a tyto údaje nepoužívá nad rámec těchto účelů.

Článek 15 (Shromažďování a používání osobních údajů) 1) Správce osobních údajů může shromažďovat osobní údaje za kterékoli z následujících okolností a používat tyto údaje v rozsahu daném účelem shromažďování:

1. je-li získán souhlas subjektu údajů;
2. existují-li v právních předpisech zvláštní ustanovení nebo je-li nutné dodržovat právní povinnosti;
3. je-li to nezbytné pro plnění povinností veřejné instituce v rámci její jurisdikce, jak je stanoví zákonné předpisy atd.;
4. je-li to nezbytně nutné k uzavření a plnění smlouvy se subjektem údajů;

([2]) Do konce přechodného období členské státy zahrnují i Spojené království, jak stanoví články 126, 127 a 132 Dohody o vystoupení Spojeného království Velké Británie a Severního Irska z Evropské unie a Evropského společenství pro atomovou energii (2019/C 384 I/01).

5. je-li to považováno za zjevně nutné pro ochranu života, zdraví nebo majetkových zájmů subjektu údajů nebo třetí strany před bezprostředním nebezpečím, pokud subjekt údajů nebo jeho zákonný zástupce není schopen vyjádřit svůj záměr nebo nelze získat předchozí souhlas kvůli neznámé adrese atd.;

6. je-li to nezbytné k dosažení oprávněného zájmu správce osobních údajů, který je zjevně nadřazen právům subjektu údajů. V takových případech je zpracování povoleno pouze v rozsahu, v němž zpracování významně souvisí s oprávněným zájmem správce osobních údajů a nepřekračuje přiměřenou míru.

Článek 18 (Omezení používání a poskytování osobních údajů za jiným než určeným účelem) 1) Správce osobních údajů nepoužívá osobní údaje nad rámec stanovený v čl. 15 odst. 1 a čl. 39-3 odst. 1 a 2 ani tyto údaje neposkytuje kterékoli třetí straně nad rámec stanovený v čl. 17 odst. 1 a 3.

2) Bez ohledu na odstavec 1, pokud se použije některý z následujících pododstavců, může správce osobních údajů použít osobní údaje nebo tyto údaje poskytnout třetí straně k jiným účelům, ledaže by tím pravděpodobně byl nekorektním způsobem narušen zájem subjektu údajů nebo třetí strany: přičemž poskytovatelů informačních a komunikačních služeb [ve smyslu čl. 2 odst. 1 bodu 3 zákona o podpoře využívání informačních a komunikačních sítí a ochraně údajů; v tomto dokumentu se použije tentýž význam], kteří zpracovávají osobní údaje uživatelů [ve smyslu čl. 2 odst. 1 bodu 4 zákona o podpoře využívání informačních a komunikačních sítí a ochraně údajů; v tomto dokumentu se použije tentýž význam], se týkají pouze první a druhý pododstavec a pátý až devátý pododstavec se použije pouze na veřejné instituce:

1. je-li od subjektu údajů získán dodatečný souhlas;

2. existují-li jiná zvláštní ustanovení právních předpisů;

3. je-li to považováno za zjevně nutné pro ochranu života, zdraví nebo majetkových zájmů subjektu údajů nebo třetí strany před bezprostředním nebezpečím, pokud subjekt údajů nebo jeho zákonný zástupce není schopen vyjádřit svůj záměr nebo nelze získat předchozí souhlas kvůli neznámé adrese;

4. zrušeno; <zákonem č. 16930, 4. února 2020>

5. není-li možné plnit povinnosti spadající do jeho jurisdikce stanovené v kterémkoli zákoně, ledaže správce osobních údajů použije osobní údaje za jiným než zamýšleným účelem nebo je poskytne třetí straně, což podléhá projednání a rozhodnutí ze strany komise;

6. je-li nezbytné poskytnout osobní údaje zahraniční vládě nebo mezinárodní organizaci za účelem plnění úmluvy nebo jiného mezinárodního závazku;

7. je-li to nezbytné pro vyšetřování trestné činnosti, obžalobu a trestní stíhání;

8. je-li to nezbytné k tomu, aby soud plnil své povinnosti související se soudním řízením;

9. je-li to nezbytné pro výkon trestu, probační a vazební opatření.

Vypuštěny odstavce 3–4.

5) Jestliže správce osobních údajů poskytne osobní údaje třetí straně za jiným než zamýšleným účelem v případech uvedených v odstavci 2, požádá správce osobních údajů příjemce takových osobních údajů, aby omezil účel a způsob použití a další nezbytné záležitosti nebo aby vypracoval potřebné záruky k zajištění bezpečnosti osobních údajů. V takových případech osoba, která takovou žádost obdrží, přijme nezbytná opatření k zajištění bezpečnosti osobních údajů.

i) Ustanovení čl. 3 odst. 1 a 2 zákona předepisují zásadu, podle níž musí správce osobních údajů shromažďovat pouze minimální osobní údaje nezbytné k oprávněnému a zákonnému naplnění účelu zpracování osobních údajů a neměl by je používat k jiným než zamýšleným účelům ([3]).

ii) Podle této zásady čl. 15 odst. 1 zákona stanoví, že pokud správce osobních údajů shromažďuje osobní údaje, mohou být tyto osobní údaje použity v rámci účelu shromažďování, a čl. 18 odst. 1 stanoví, že osobní údaje by neměly být použity nad rámec účelu shromažďování nebo poskytnuty třetí straně.

([3]) Vzhledem k tomu, že tato ustanovení stanoví obecné zásady, které se vztahují na jakékoli zpracování osobních údajů, včetně případů, kdy je takové zpracování výslovně upraveno jinými zákony, objasnění v tomto oddíle platí také v případě, kdy jsou osobní údaje zpracovávány na základě jiných zákonů (viz např. čl. 15 odst. 1 zákona o úvěrových informacích, který na tato ustanovení konkrétně odkazuje).

iii) Přestože ve výjimečných případech ([4]) popsaných v pododstavcích čl. 18 odst. 2 zákona mohou být osobní údaje použity pro jiné než zamýšlené účely nebo poskytnuty třetí osobě, musí být vyžadováno, aby byl omezen účel nebo způsob použití, aby mohly být osobní údaje zpracovány bezpečně podle odstavce 5, nebo aby byla přijata opatření nezbytná k zajištění bezpečnosti osobních údajů.

iv) Výše uvedená ustanovení se použijí stejnou měrou na zpracování všech osobních údajů přijatých ze třetí země v oblasti spadající do korejské jurisdikce, bez ohledu na státní příslušnost subjektu údajů.

v) Pokud například správce osobních údajů v EU předá osobní údaje korejskému správci osobních údajů v souladu s rozhodnutím Evropské komise o odpovídající ochraně, považuje se účel předání osobních údajů uplatněný správcem osobních údajů v EU za účel shromažďování osobních údajů korejského správce osobních údajů a v takových případech může korejský správce osobních údajů dané osobní údaje použít nebo je poskytnout třetí straně v mezích daných účelem shromažďování, s výhradou výjimečných případů popsaných v pododstavcích čl. 18 odst. 2 zákona.

2. **Omezení dalšího předávání osobních údajů (čl. 17 odst. 3 a 4, článek 18 zákona)**

<Zákon o ochraně osobních údajů

(zákon č. 16930 ve znění částečně pozměněném dne 4. února 2020)>

článek 17 (Poskytování osobních údajů) 1) Vypuštěno.

2) Jestliže získá souhlas podle odst. 1 prvního pododstavce, informuje správce osobních údajů subjekt údajů o níže uvedených záležitostech. Totéž platí, dojde-li ke změně kteréhokoli z těchto prvků:

1. příjemce osobních údajů;
2. účel, za nímž příjemce osobních údajů takové údaje používá;
3. zvláštní rysy osobních údajů, které mají být poskytnuty;
4. období, po které příjemce uchovává a používá osobní údaje;
5. skutečnost, že subjekt údajů je oprávněn souhlas odepřít, a případná znevýhodnění vyplývající z odepření souhlasu.

3) Správce osobních údajů informuje subjekt údajů o záležitostech uvedených v odstavci 2 a získá souhlas subjektu údajů k poskytnutí osobních údajů třetí straně v zahraničí a neuzavře smlouvu o přeshraničním předání osobních údajů v rozporu s tímto zákonem.

4) Správce osobních údajů může poskytnout osobní údaje bez souhlasu subjektu údajů v rozsahu přiměřeně souvisejícím s účely, pro které byly osobní údaje původně shromážděny, v souladu se záležitostmi předepsanými prezidentskou vyhláškou a s přihlédnutím k tomu, zda je tím subjekt údajů znevýhodněn, zda byla provedena nezbytná opatření k zajištění bezpečnosti, například šifrování, atd.

※ Článek 18 viz strany 3, 4 a 5.

< **Prováděcí vyhláška k zákonu o ochraně osobních údajů**

([Datum začátku použitelnosti 5. února 2021.] [prezidentská vyhláška č. 30892, 4. srpna 2020, kterou se mění další zákony])>

Článek 14-2 (Standardy pro další použití / poskytování osobních údajů atd.)

1) Pokud správce osobních údajů používá nebo poskytuje osobní údaje (dále jen „další použití nebo poskytnutí osobních údajů“) bez souhlasu subjektu údajů v souladu s čl. 15 odst. 3 zákona nebo s čl. 17 odst. 4 zákona, správce osobních údajů zváží následující:

1. zda použití nebo poskytnutí přiměřeně souvisí s původním účelem, za nímž byly osobní údaje shromážděny;
2. zda je další použití nebo poskytnutí osobních údajů předvídatelné s ohledem na okolnosti, za kterých byly osobní údaje shromážděny, a na postupy zpracování;
3. zda další použití nebo poskytnutí osobních údajů nekorektním způsobem neporušuje zájmy subjektu údajů a dále
4. zda byla přijata opatření nezbytná k zajištění bezpečnosti, jako je pseudonymizace nebo šifrování.

([4]) Na poskytovatele informačních a komunikačních služeb se použije pouze čl. 18 odst. 2 první a druhý pododstavec. Pátý až devátý pododstavec se použije pouze na veřejné instituce.

2) Správce osobních údajů předem zveřejní kritéria pro posuzování záležitostí uvedených v pododstavcích odstavce 1 v koncepci ochrany soukromí podle čl. 30 odst. 1 zákona a pověřenec pro ochranu soukromí podle čl. 31 odst. 1 zákona zkontroluje, zda správce osobních údajů používá nebo poskytuje další osobní údaje v souladu s příslušnými normami.

i) Pokud správce osobních údajů poskytne osobní údaje třetí straně v zahraničí, musí předem informovat subjekty údajů o všech záležitostech uvedených v čl. 17 odst. 2 zákona a musí získat jejich souhlas, vyjma případů spadajících do oblasti působnosti odstavce 1 nebo 2. Žádná smlouva o přeshraničním poskytnutí osobních údajů nesmí být uzavřena v rozporu s tímto zákonem.

(1) Pokud jsou osobní údaje poskytnuty v rozsahu přiměřeně souvisejícím s původním účelem shromažďování podle čl. 17 odst. 4 zákona. Situace, kdy lze toto ustanovení použít, jsou však omezeny na případy, kdy jsou splněny standardy pro další použití a poskytnutí osobních údajů stanovené v článku 14-2 prováděcí vyhlášky. Kromě toho musí správce osobních údajů zvážit, zda může poskytnutí osobních údajů subjekty údajů znevýhodnit a zda přijal nezbytná opatření k zajištění bezpečnosti, například šifrování.

(2) Pokud mohou být osobní údaje poskytnuty třetí osobě ve výjimečných případech uvedených v čl. 18 odst. 2 zákona (viz strany 3–5). Avšak ani v takových případech nelze osobní údaje třetí straně poskytnout, pokud by poskytnutí takových osobních údajů pravděpodobně nekorektním způsobem porušilo zájmy subjektu údajů nebo třetí strany. Kromě toho musí poskytovatel osobních údajů požádat příjemce osobních údajů, aby omezil účel nebo způsob použití osobních údajů nebo přijal opatření nezbytná k zajištění jejich bezpečnosti tak, aby mohly být osobní údaje zpracovány bezpečným způsobem.

ii) Pokud jsou osobní údaje poskytnuty třetí straně v zahraničí, nemusí jim být zajištěna úroveň ochrany zaručená korejským zákonem o ochraně osobních údajů kvůli rozdílům v systémech ochrany osobních údajů v různých zemích. V souladu s tím budou takové případy považovány za „případy, kdy může být subjekt údajů znevýhodněn“ ve smyslu čl. 17 odst. 4 zákona nebo „případy, kdy je nekorektním způsobem porušen zájem subjektu údajů nebo třetí strany“ ve smyslu čl. 18 odst. 2 zákona a článku 14-2 prováděcí vyhlášky k tomuto zákonu ([5]). Aby splnil požadavky těchto ustanovení, musí tudíž správce osobních údajů a třetí strana výslovně zajistit úroveň ochrany rovnocennou ochraně podle zákona, včetně záruky výkonu práv subjektu údajů v právně závazných dokumentech, jako jsou smlouvy, a to i v případě předání osobních údajů do zahraničí.

3. **Oznámení o údajích, pokud osobní údaje nebyly získány od subjektu údajů (článek 20 zákona)**

<Zákon o ochraně osobních údajů

(zákon č. 16930 ve znění částečně pozměněném dne 4. února 2020)>

Článek 20 (Oznámení o zdrojích atd. osobních údajů shromážděných od třetích stran) 1) Jestliže správce osobních údajů zpracovává osobní údaje shromážděné od třetích stran, tento správce osobních údajů na žádost subjektu údajů neprodleně sdělí subjektu údajů tyto informace:

1. zdroj shromážděných osobních údajů;

2. účel zpracování osobních údajů;

3. skutečnost, že subjekt údajů je oprávněn požadovat pozastavení zpracování osobních údajů, jak je stanoveno v článku 37.

2) Nehledě na odstavec 1, pokud správce osobních údajů splňující kritéria předepsaná prezidentskou vyhláškou s přihlédnutím k druhům a množství zpracovávaných osobních údajů, počtu zaměstnanců, objemu tržeb atd. shromažďuje osobní údaje od třetích stran a zpracovává je podle čl. 17 odst. 1 bodu 1, sdělí správce osobních údajů subjektu údajů informace uvedené v odstavci 1: přičemž toto ustanovení se nepoužije, pokud informace shromážděné správcem osobních údajů neobsahují žádné osobní údaje, například kontaktní údaje, prostřednictvím nichž lze subjektu údajů podat oznámení.

([5]) Podle čl. 18 odst. 2 bodu 2 zákona o ochraně osobních údajů to platí i v případě, že jsou osobní údaje zpřístupněny třetím stranám v zahraničí na základě ustanovení jiných zákonů (například zákona o úvěrových informacích).

3) Potřebné záležitosti týkající se času, způsobu a postupu podávání oznámení subjektu údajů podle hlavní věty odstavce 2 stanoví prezidentská vyhláška.

4) Odstavec 1 a hlavní ustanovení odstavce 2 se nepoužijí v žádné z těchto situací: přičemž tomu tak bude pouze v případě, že tato ustanovení budou zjevně nadřazena právům subjektů údajů podle tohoto zákona:

1. pokud jsou osobní údaje, které jsou předmětem žádosti o oznámení, obsaženy v souborech osobních informací uvedených v kterémkoli z pododstavců čl. 32 odst. 2;

2. pokud je pravděpodobné, že takové oznámení způsobí újmu na životě nebo zdraví jakékoli jiné osoby nebo nekorektním způsobem způsobí škodu na majetku a jiných zájmech kterékoli jiné osoby.

(i) Pokud správce osobních údajů obdrží osobní údaje předané z EU na základě rozhodnutí EU o odpovídající ochraně ([6]), musí bez zbytečného odkladu, v každém případě nejpozději do jednoho měsíce od předání, sdělit subjektu údajů informace uvedené v bodech 1 až 5 níže.

(1) Jméno a kontaktní údaje osob, které osobní údaje předávají a přijímají.

(2) Položky nebo kategorie předávaných osobních údajů.

(3) Účel shromažďování a používání osobních údajů (jak je stanoven vývozcem údajů podle bodu 1 tohoto oznámení).

(4) Doba uchovávání osobních údajů.

(5) Informace o právech subjektu údajů v souvislosti se zpracováním osobních údajů, o způsobu a postupu výkonu práv a o případných znevýhodněních, pokud výkon práv vede ke znevýhodněním.

(ii) Pokud správce osobních údajů poskytne osobní údaje uvedené v bodě i) třetí straně v Korejské republice nebo v zahraničí, musí subjektu údajů sdělit informace podle bodů 1 až 5 dříve, než budou osobní údaje poskytnuty.

(1) Jméno a kontaktní údaje osob, které osobní údaje poskytují a přijímají.

(2) Položky nebo kategorie poskytnutých osobních údajů.

(3) Země, do které budou osobní údaje poskytnuty, předpokládané datum a způsob jejich poskytnutí (s omezením na případy, kdy budou osobní údaje poskytnuty třetí straně v zahraničí).

(4) Účel sledovaný poskytovatelem osobních údajů a právní základ poskytnutí osobních údajů.

(5) Informace o právech subjektu údajů v souvislosti se zpracováním osobních údajů, o způsobu a postupu výkonu práv a o případných znevýhodněních, pokud výkon práv vede ke znevýhodněním.

(iii) Správce osobních údajů nesmí použít body i) nebo ii) v žádném z případů uvedených v bodech 1 až 4 níže.

(1) Pokud jsou osobní údaje, které je třeba oznámit, obsaženy v některém z následujících souborů osobních údajů uvedených v čl. 32 odst. 2 zákona, za předpokladu, že jsou zájmy chráněné tímto ustanovením zjevně nadřazeny právům subjektu údajů, a pouze pokud by oznámení ohrozilo sledování dotyčných zájmů, například by došlo k ohrožení probíhajících vyšetřování trestných činů nebo ohrožení národní bezpečnosti.

(2) Pokud a dokud je pravděpodobné, že oznámení způsobí újmu na životě nebo zdraví jakékoli jiné osoby nebo nekorektním způsobem poškodí majetkové zájmy jiné osoby, pokud jsou tato práva nebo zájmy zjevně nadřazeny právům subjektu údajů.

(3) Pokud subjekt údajů již má v držení údaje, které musí správce osobních údajů oznámit podle bodů i) nebo ii).

(4) Pokud správce osobních údajů nemá žádné kontaktní údaje subjektu údajů nebo pokud kontaktování subjektu údajů vyžaduje nadměrné úsilí, a to i v souvislosti se zpracováním za podmínek stanovených v oddíle 3 zákona o ochraně osobních údajů. Při určování toho, zda je možné kontaktovat subjekt údajů nebo zda to vyžaduje nadměrné úsilí, by měla být vzata v úvahu možnost spolupracovat s vývozcem údajů v EU.

([6]) Povinnosti podle bodů i), ii) a iii) platí stejně, pokud správce, který obdrží osobní údaje předané z EU na základě postupů podle rozhodnutí o odpovídající ochraně, zpracovává tyto údaje podle jiných zákonů, například podle zákona o úvěrových informacích.

4. **Rozsah použití zvláštní výjimky na zpracování pseudonymizovaných údajů (články 28-2, 28-3, 28-4, 28-5, 28-6 a 28-7, článek 3 a článek 58-2 zákona)**

<Zákon o ochraně osobních údajů

(zákon č. 16930 ve znění částečně pozměněném dne 4. února 2020)>

Kapitola III Zpracování osobních údajů

ODDÍL 3 Zvláštní případy týkající se pseudonymních údajů

Článek 28-2 (Zpracování pseudonymních údajů) 1) Správce osobních údajů může zpracovávat pseudonymizované údaje bez souhlasu subjektů údajů pro účely statistiky, vědeckého výzkumu a archivace ve veřejném zájmu atd.

2) Při poskytování pseudonymizovaných údajů třetí straně podle odstavce 1 nesmí správce osobních údajů zahrnout údaje, které lze použít k identifikaci určité osoby.

Článek 28-3 (Omezení kombinace pseudonymních údajů) 1) Bez ohledu na článek 28-2 provádí kombinování pseudonymizovaných údajů zpracovávaných různými správci osobních údajů pro účely statistiky, vědeckého výzkumu a archivace ve veřejném zájmu atd. specializovaná instituce určená Komisí pro ochranu údajů nebo ředitelem související ústřední správní agentury.

2) Správce osobních údajů, který hodlá zveřejnit zkombinované údaje mimo organizaci, která tyto údaje zkombinovala, musí po zpracování údajů do pseudonymizované podoby nebo podoby uvedené v článku 58-2 získat souhlas ředitele specializované instituce.

3) Nezbytné záležitosti včetně postupů a metod kombinování podle odstavce 1, norem a postupů pro jmenování nebo zrušení jmenování vedení specializované instituce a dohledu nad touto institucí a norem a postupů pro vývoz a schválení podle odstavce 2 stanoví prezidentská vyhláška.

Článek 28-4 (Povinnost přijmout bezpečnostní opatření pro pseudonymní údaje) 1) Při zpracování pseudonymizovaných údajů přijme správce osobních údajů taková technická, organizační a fyzická opatření, jako je samostatné ukládání a správa dalších údajů potřebných k obnovení údajů do původního stavu, nezbytná k zajištění bezpečnosti podle prezidentské vyhlášky, aby nemohlo dojít ke ztrátě, odcizení, vyzrazení, padělání, pozměnění nebo poškození osobních údajů.

2) Správce osobních údajů, který hodlá zpracovávat pseudonymizované údaje, vyhotoví a povede záznamy týkající se záležitostí předepsaných prezidentskou vyhláškou, včetně účelu zpracování pseudonymizovaných údajů, a třetí strany, která je příjemcem údajů při poskytování pseudonymizovaných údajů, pro účely správy zpracování pseudonymizovaných údajů.

Článek 28-5 (Zakázané úkony při zpracování pseudonymizovaných údajů) 1) Nikdo nesmí zpracovávat pseudonymizované údaje za účelem identifikace určité osoby.

2) Pokud jsou při zpracování pseudonymizovaných údajů generovány údaje identifikující určitou osobu, správce osobních údajů ukončí zpracování daných údajů a okamžitě tyto údaje extrahuje a zničí.

Článek 28-6 (Uložení správních pokut za zpracování pseudonymizovaných údajů) 1) Komise může správci údajů, který zpracovával údaje za účelem identifikace konkrétní osoby v rozporu s čl. 28–5 odst. 1, uložit pokutu, která činí nejvýše tři setiny celkových tržeb: přičemž v případě nulových tržeb nebo obtíží při jejich výpočtu může být správci údajů uložena pokuta v maximální výši 400 milionů wonů nebo tří setin hodnoty kapitálu, podle toho, která částka je vyšší.

2) Na záležitosti nezbytné k uložení a výběru správních pokut se použije obdobně čl. 34-2 odst. 3 až 5.

Článek 28-7 (Oblast působnosti) @Články 20, 21, 27, čl. 34 odst. 1, články 35 až 37, 39-3, 39-4 a články 39-6 až 39-8 se na pseudonymizované údaje nepoužijí.

Kapitola I Všeobecná ustanovení

Článek 3 (Zásady ochrany osobních údajů) 1) Správce osobních údajů výslovně stanoví účely, pro které jsou osobní údaje zpracovávány, a shromažďuje osobní údaje zákonným a korektním způsobem v minimálním rozsahu nezbytném pro tyto účely.

2) Správce osobních údajů zpracovává osobní údaje vhodným způsobem, který je nezbytný pro účely, pro které jsou osobní údaje zpracovávány, a tyto údaje nepoužívá nad rámec těchto účelů.

3) Správce osobních údajů zajistí, aby osobní údaje byly přesné, úplné a aktuální v míře nezbytné ve vztahu k účelům, pro které jsou tyto osobní údaje zpracovávány.

4) Správce osobních údajů zajišťuje bezpečnou správu osobních údajů podle metod zpracování, druhů osobních údajů atd., s přihlédnutím k možnosti porušení práv subjektu údajů a k závažnosti příslušných rizik.

5) Správce osobních údajů zveřejní své zásady ochrany soukromí a další záležitosti související se zpracováním osobních údajů a zaručí práva subjektu údajů, jako je právo na přístup k jeho osobním údajům.

6) Správce osobních údajů zpracovává osobní údaje způsobem, který minimalizuje možnost narušení soukromí subjektu údajů.

7) Je-li stále možné naplnit účely shromažďování osobních údajů zpracováním anonymizovaných nebo pseudonymizovaných osobních údajů, správce osobních údajů se bude snažit zpracovávat osobní údaje s využitím anonymizace, pokud je anonymizace možná, nebo pseudonymizace, pokud nelze účely shromažďování osobních údajů naplnit pomocí anonymizace.

8) Správce osobních údajů se snaží získat důvěru subjektů údajů dodržováním a plněním úkolů a povinností stanovených tímto zákonem a ostatními souvisejícími právními předpisy.

Kapitola IX Doplňková ustanovení

Článek 58-2 (Vynětí z použití) Tento zákon se nevztahuje na údaje, které již v kombinaci s jinými údaji neidentifikují určitou osobu, za předpokladu přiměřeného zohlednění času, nákladů, technologie atd. <Tento článek je nově vložen zákonem č. 16930 ze dne 4. února 2020>

i) Kapitola III, oddíl 3 Zvláštní případy týkající se pseudonymních údajů (články 28-2 až 28-7) umožňuje zpracování pseudonymizovaných údajů bez souhlasu subjektu údajů za účelem sestavování statistik, vědeckého výzkumu, uchovávání veřejných záznamů atd. (článek 28-2), v takových případech je však nutné zajistit odpovídající záruky a zákazy nezbytné k ochraně práv subjektů údajů (články 28-4 a 28-5), osobám, které se dopustí jejich porušení, mohou být uloženy pokuty (článek 28-6), a některé záruky jinak dostupné v rámci zákona o ochraně osobních údajů se nepoužijí (článek 28-7).

ii) Tato ustanovení se nepoužijí na případy, kdy jsou pseudonymizované údaje zpracovávány pro jiné účely než pro sestavování statistik, vědecký výzkum, uchovávání veřejných záznamů atd. Například jsou-li osobní údaje jednotlivce z EU, které byly předány do Koreje na základě rozhodnutí Evropské komise o odpovídající ochraně, pseudonymizovány pro jiné účely než pro účely sestavování statistik, vědeckého výzkumu, uchovávání veřejných záznamů atd., zvláštní ustanovení kapitoly III oddílu 3 se nepoužijí ([7]).

iii) Pokud správce osobních údajů zpracovává pseudonymizované údaje pro účely sestavování statistik, vědeckého výzkumu, uchovávání veřejných záznamů atd. a pokud nebyly pseudonymizované údaje zničeny, jakmile byl splněn konkrétní účel zpracování v souladu s článkem 37 ústavy a článkem 3 zákona (Zásady ochrany osobních údajů), správce osobních údajů anonymizuje údaje, aby zajistil, že již nebudou identifikovat konkrétní osobu, a to samostatně nebo v kombinaci s jinými údaji, za předpokladu přiměřeného zohlednění času, nákladů, technologie atd. v souladu s článkem 58-2 zákona o ochraně osobních údajů.

5. **Nápravná opatření atd. (čl. 64 odst. 1, 2 a 4 zákona)**

<Zákon o ochraně osobních údajů

(zákon č. 16930 ve znění částečně pozměněném dne 4. února 2020)>

Článek 64 (Nápravná opatření) 1) Má-li Komise pro ochranu údajů za to, že existuje závažný důvod se domnívat, že došlo k porušení předpisů v oblasti osobních údajů, a nečinnost pravděpodobně způsobí obtížně napravitelnou škodu, může subjektu, který se dopustil porušení tohoto zákona (vyjma ústředních správních agentur, orgánů místní správy, Národního shromáždění, soudu, Ústavního soudu a Národní volební komise) nařídit, aby přijal některá z těchto opatření:

1. ukončit porušování předpisů týkající se osobních údajů;

2. dočasně pozastavit zpracování osobních údajů;

([7]) Podobně se výjimka podle článku 40-3 zákona o úvěrových informacích použije pouze na zpracování pseudonymizovaných úvěrových informací pro účely sestavování statistik, vědeckého výzkumu a uchovávání veřejných záznamů.

3. jiná opatření nezbytná k ochraně osobních údajů a k předcházení porušení zabezpečení osobních údajů.

2) Pokud má ředitel související ústřední správní agentury za to, že existuje závažný důvod se domnívat, že došlo k porušení zabezpečení osobních údajů, a nečinnost pravděpodobně způsobí obtížně napravitelnou škodu, může nařídit správci osobních údajů, aby přijal některá z opatření uvedených v odstavci 1 v souladu s právními předpisy v rámci příslušné jurisdikce této ústřední správní agentury.

4) Pokud se ústřední správní agentura, orgán místní správy, Národní shromáždění, soud, Ústavní soud nebo Národní volební komise dopustí porušení tohoto zákona, může Komise pro ochranu údajů doporučit řediteli příslušné agentury, aby přijal kterékoli z opatření uvedených v odstavci 1. V takových případech je agentura po obdržení doporučení povinna toto doporučení dodržet, pokud neexistují mimořádné okolnosti.

i) Zaprvé soudní precedenty ([8]) ([9]) vykládají „obtížně napravitelnou škodu“ jako situaci, která by mohla způsobit narušení osobních práv nebo soukromí jednotlivce.

ii) Tudíž „závažný důvod se domnívat, že došlo k porušení předpisů v oblasti osobních údajů, a nečinnost pravděpodobně způsobí obtížně napravitelnou škodu“ podle čl. 64 odst. 1 a 2 odkazuje na případy, kdy se má za to, že porušení zákona pravděpodobně poruší práva a svobodu jednotlivců v souvislosti s osobními údaji. Toto ustanovení bude použitelné vždy, když dojde k porušení jakýchkoli zásad, práv a povinností uvedených v právních předpisech o ochraně osobních údajů ([10]).

iii) Podle čl. 64 odst. 4 zákona o ochraně osobních údajů jde o opatření ve věci „porušení tohoto zákona“, tj. opatření směřující proti porušení zákona o ochraně osobních údajů.

Ústřední správní agentura atd. jako orgán veřejné správy vázaný zásadami právního státu nesmí porušovat žádný právní předpis a je povinna přijmout nápravná opatření, včetně okamžitého zastavení jednání a náhrady škody ve výjimečném případě, kdy byl nezákonný čin přesto spáchán.

I bez jakéhokoli zásahu Komise pro ochranu osobních údajů podle čl. 64 odst. 4 zákona o ochraně osobních údajů musí tudíž ústřední správní agentura atd. přijmout nápravné opatření proti porušením právních předpisů, pokud se dozví o jakémkoli porušení právních předpisů.

Zejména pokud Komise pro ochranu osobních údajů doporučila nápravné opatření, bude ústřední správní agentuře atd. obvykle objektivně jasné, že porušila zákon. Aby tedy odůvodnila, proč se domnívá, že by doporučení Komise pro ochranu osobních údajů nemělo být dodrženo, musí ústřední správní agentura atd. předložit jasné důvody, které mohou prokázat, že právní předpisy neporušila. Doporučení musí být dodrženo, pokud Komise pro ochranu osobních údajů nerozhodne, že k tomu skutečně není důvod.

S ohledem na to musí být „mimořádné okolnosti“ podle čl. 64 odst. 4 zákona o ochraně osobních údajů přísně omezeny na mimořádné okolnosti, za nichž existují jasné důvody k tomu, aby ústřední správní agentury atd. prokázaly, že „tento zákon ve skutečnosti nebyl porušen“, například „případy, kdy existují mimořádné (skutkové nebo právní) okolnosti“, o nichž Komise pro ochranu osobních údajů při svém doporučení původně nevěděla, a tato komise dojde k závěru, že k žádnému porušení zákona skutečně nedošlo.

6. **Použití zákona o ochraně osobních údajů na zpracování osobních údajů pro účely národní bezpečnosti včetně vyšetřování protiprávních jednání a vymáhání v souladu se zákonem o ochraně osobních údajů (článek 7-8, článek 7-9, článek 58, článek 3, článek 4 a článek 62 zákona o ochraně osobních údajů)**

<Zákon o ochraně osobních údajů

(zákon č. 16930 ve znění částečně pozměněném dne 4. února 2020)>

Článek 7-8 (Činnost Komise pro ochranu osobních údajů) 1) Komise pro ochranu osobních údajů vykonává tyto činnosti: […]

3. záležitosti týkající se vyšetřování porušení práv subjektů údajů a vyplývajících opatření;

4. vyřizování stížností nebo nápravné postupy související se zpracováním osobních údajů a mediací ve sporech týkajících se osobních údajů;

[…]

([8]) (Rozsudek Nejvyššího soudu 97Da10215,10222 ze dne 26. ledna 1999.) Jsou-li prostřednictvím sdělovacích prostředků zpřístupněny údaje týkající se trestné činnosti obviněného, pravděpodobně to způsobí nenapravitelnou duševní a fyzickou škodu nejen oběti, tj. žalobci, ale také lidem v jejím okolí, včetně rodin.

([9]) (Rozsudek vrchního soudu v Soulu 2006Na92006 ze dne 16. ledna 2008.) Je-li zveřejněn hanlivý článek, pravděpodobně to způsobí dotčené osobě závažnou nenapravitelnou škodu.

([10]) Tytéž zásady, jaké jsou stanoveny v bodě ii), se vztahují na článek 45-4 zákona o úvěrových informacích.

Článek 7-9 (Záležitosti podléhající projednání a rozhodnutí Komisí pro ochranu osobních údajů) 1) Komise pro ochranu osobních údajů projednává a rozhoduje tyto záležitosti: […]

5. záležitosti týkající se výkladu a fungování práva v oblasti ochrany osobních údajů;

[…]

Článek 58 (Částečné vyloučení použití) 1) Kapitoly III až VII se nepoužijí na žádné z těchto osobních údajů:

1. osobní údaje shromážděné podle zákona o statistice pro účely zpracování veřejnými institucemi;

2. osobní údaje shromážděné nebo požadované pro účely analýzy informací souvisejících s národní bezpečností;

3. dočasně zpracovávané osobní údaje v případech, kde je to naléhavě nutné pro veřejnou bezpečnost a ochranu, veřejné zdraví atd.;

4. osobní údaje shromážděné nebo používané pro vlastní účely tiskových zpráv, misijní činnosti náboženských organizací, resp. nominace kandidátů politickými stranami.

[odstavce 2 a 3 vypuštěny]

4) V případě zpracování osobních údajů podle odstavce 1 správce osobních údajů zpracovává osobní údaje v minimálním rozsahu nezbytném k dosažení zamýšleného účelu po minimální dobu; přijme také nezbytná opatření, například technické, řídicí a fyzické záruky, individuální řešení stížností a další nezbytná opatření pro bezpečnou správu a náležité zpracování takových osobních údajů.

Článek 3 (Zásady ochrany osobních údajů) 1) Správce osobních údajů výslovně stanoví účely, pro které jsou osobní údaje zpracovávány, a shromažďuje osobní údaje zákonným a korektním způsobem v minimálním rozsahu nezbytném pro tyto účely.

2) Správce osobních údajů zpracovává osobní údaje vhodným způsobem, který je nezbytný pro účely, pro které jsou osobní údaje zpracovávány, a tyto údaje nepoužívá nad rámec těchto účelů.

3) Správce osobních údajů zajistí, aby osobní údaje byly přesné, úplné a aktuální v míře nezbytné ve vztahu k účelům, pro které jsou tyto osobní údaje zpracovávány.

4) Správce osobních údajů zajišťuje bezpečnou správu osobních údajů podle metod zpracování, druhů osobních údajů atd., s přihlédnutím k možnosti porušení práv subjektu údajů a k závažnosti příslušných rizik.

5) Správce osobních údajů zveřejní své zásady ochrany soukromí a další záležitosti související se zpracováním osobních údajů a zaručí práva subjektu údajů, jako je právo na přístup k jeho osobním údajům.

6) Správce osobních údajů zpracovává osobní údaje způsobem, který minimalizuje možnost narušení soukromí subjektu údajů.

7) Je-li stále možné naplnit účely shromažďování osobních údajů zpracováním anonymizovaných nebo pseudonymizovaných osobních údajů, správce osobních údajů se musí snažit zpracovávat osobní údaje s využitím anonymizace, pokud je anonymizace možná, nebo pseudonymizace, pokud nelze účely shromažďování osobních údajů naplnit pomocí anonymizace.

8) Správce osobních údajů se snaží získat důvěru subjektů údajů dodržováním a plněním úkolů a povinností stanovených tímto zákonem a ostatními souvisejícími právními předpisy.

Článek 4 (Práva subjektů údajů) Subjekt údajů má v souvislosti se zpracováním jeho osobních údajů tato práva:

1. právo být informován o zpracování takových osobních údajů;

2. právo rozhodnout, zda udělí, či neudělí souhlas se zpracováním takových osobních údajů, a určit rozsah tohoto souhlasu;

3. právo potvrdit, zda jsou osobní údaje zpracovávány, či nikoli, a požadovat přístup (včetně poskytnutí kopií; na ty se použijí tatáž ustanovení) k těmto osobním údajům;

4. právo pozastavit zpracování těchto osobních údajů a požadovat jejich opravu, výmaz a zničení;

5. právo na přiměřenou náhradu jakékoli škody vzniklé v důsledku zpracování takových osobních údajů, a to prostřednictvím rychlého a spravedlivého řízení.

Článek 62 (Oznamování porušení právních předpisů) 1) Kdokoli, jehož práva nebo zájmy týkající se jeho osobních údajů jsou porušeny při zpracování osobních údajů správcem osobních údajů, může toto porušení oznámit Komisi pro ochranu osobních údajů.

2) Komise pro ochranu osobních údajů může určit specializovanou instituci, která bude účinně přijímat a zpracovávat oznámení o nárocích podle odstavce 1, jak stanoví prezidentská vyhláška. V takových případech tato specializovaná instituce zřídí a bude provozovat telefonické kontaktní centrum pro záležitosti týkající se porušení ochrany osobních údajů (dále jen „kontaktní centrum pro ochranu soukromí").

3) Kontaktní centrum pro ochranu soukromí plní tyto povinnosti:

1. přijímat oznámení o nárocích a poskytovat konzultace týkající se zpracování osobních údajů;

2. vyšetřovat a potvrzovat incidenty a vyslechnout názory příslušných stran;

3. povinnosti související s prvním a druhým pododstavcem.

4) Komise pro ochranu osobních údajů může v případě potřeby vyslat svého úředníka do specializované instituce jmenované podle odstavce 2 na základě článku 32-4 zákona o státních úřednících, aby účinně vyšetřoval a potvrzoval incidenty podle odst. 3 bodu 2.

i) Shromažďování osobních údajů pro účely národní bezpečnosti je upraveno zvláštními právními předpisy, které zmocňují příslušné orgány (např. Národní zpravodajskou službu) provádět odposlech komunikace nebo požadovat zpřístupnění údajů, a to za určitých podmínek a záruk (dále jen „právní předpisy v oblasti národní bezpečnosti"). Tyto právní předpisy v oblasti národní bezpečnosti zahrnují například zákon o ochraně důvěrnosti komunikací, zákon o boji proti terorismu na ochranu občanů a veřejné bezpečnosti nebo zákon o telekomunikacích. Shromažďování a další zpracování osobních údajů musí navíc splňovat požadavky zákona o ochraně osobních údajů. V tomto ohledu čl. 58 odst. 1 bod 2 zákona o ochraně osobních údajů stanoví, že kapitoly III až VII se nepoužijí na osobní údaje shromážděné nebo požadované pro účely analýzy informací souvisejících s národní bezpečností. Tato částečná výjimka se tedy použije na zpracování osobních údajů pro účely národní bezpečnosti.

Současně se na zpracování takových osobních údajů vztahuje kapitola I (Všeobecná ustanovení), kapitola II (Stanovení zásad ochrany osobních údajů atd.), kapitola VIII (Hromadná žaloba týkající se porušení ochrany údajů), kapitola IX (Doplňková ustanovení) a kapitola X (Ustanovení o sankcích) zákona o ochraně osobních údajů. To zahrnuje obecné zásady ochrany údajů stanovené v článku 3 (Zásady ochrany osobních údajů) a individuální práva zaručená článkem 4 zákona o ochraně osobních údajů (Práva subjektů údajů).

Kromě toho čl. 58 odst. 4 zákona o ochraně osobních údajů stanoví, že tyto údaje musí být zpracovávány v minimálním rozsahu nezbytném pro dosažení zamýšleného účelu a po minimální dobu, a požaduje také, aby správce osobních údajů zavedl nezbytná opatření k zajištění bezpečné správy údajů a náležitého zpracování, jako jsou technické, řídicí a fyzické záruky, jakož i opatření pro náležité vyřizování individuálních stížností.

A konečně se použijí také ustanovení upravující úkoly a pravomoci Komise pro ochranu osobních údajů (včetně článku 60-65 zákona o ochraně osobních údajů o vyřizování stížností a přijímání doporučení a nápravných opatření) a také ustanovení o správních a trestních sankcích (článek 70 a násl. zákona o ochraně osobních údajů). Podle čl. 7-8 odst. 1 bodu 3 a 4 a čl. 7-9 odst. 1 bodu 5 zákona o ochraně osobních údajů se tyto vyšetřovací a nápravné pravomoci, a to i pokud jsou uplatněny v rámci vyřizování stížností, týkají i případných porušení pravidel obsažených ve zvláštních právních předpisech, kterými se stanoví omezení a záruky týkající se shromažďování osobních údajů, jako jsou právní předpisy v oblasti národní bezpečnosti. Vzhledem k požadavkům čl. 3 odst. 1 zákona o ochraně osobních údajů na zákonné a korektní shromažďování osobních údajů představuje takové porušení právních předpisů porušení „tohoto zákona" ve smyslu článků 63 a 64, což Komisi pro ochranu osobních údajů umožňuje provádět vyšetřování a přijímat nápravná opatření ([11]). Výkon těchto pravomocí ze strany Komise pro ochranu osobních údajů doplňuje, ale nenahrazuje pravomoci Národní komise pro lidská práva podle zákona o Národní komisi pro lidská práva.

Uplatňování základních zásad, práv a povinností podle zákona o ochraně osobních údajů na zpracování osobních údajů pro účely národní bezpečnosti odráží záruky zakotvené v ústavě, pokud jde o ochranu práva jednotlivce na kontrolu jeho osobních údajů. Jak uznal Ústavní soud, toto právo zahrnuje právo jednotlivce ([12]) „osobně rozhodnout, kdy, vůči komu nebo kým a do jaké míry budou jeho údaje zpřístupněny nebo použity. Jde o základní právo ([13]), […], které má chránit osobní svobodu rozhodování před rizikem způsobeným rozšířením funkcí státu a informační a komunikační technologií." Jakékoli omezení tohoto práva, například je-li nezbytné pro ochranu národní bezpečnosti, vyžaduje vyvážení práv a zájmů jednotlivce vůči příslušnému veřejnému zájmu a nesmí se dotknout podstaty práva (čl. 37 odst. 2 ústavy).

([11]) Nápravná opatření podle článku 64 viz také oddíl 5 výše.
([12]) Rozsudek Ústavního soudu 99HunMa513 a 2004HunMa190 ze dne 26. května 2005.
([13]) Rozsudek Ústavního soudu 2003HunMa282 ze dne 21. července 2005.

Při zpracování osobních údajů pro účely národní bezpečnosti proto správce (např. Národní zpravodajská služba) mimo jiné:

1) výslovně specifikuje účely, pro které jsou osobní údaje zpracovávány, a shromažďuje osobní údaje zákonným a korektním způsobem v minimálním rozsahu nezbytném pro tyto účely (čl. 3 odst. 1 zákona o ochraně osobních údajů); konkrétně shromažďuje a dále zpracovává osobní údaje pouze pro účely plnění povinností podle příslušných právních předpisů, jako je zákon o Národní zpravodajské službě;

2) zpracovává osobní údaje v minimálním rozsahu a po minimální dobu nezbytnou k dosažení zamýšleného účelu (čl. 58 odst. 4 zákona o ochraně osobních údajů); po dosažení účelu zpracování správce osobní údaje nevratně zničí, ledaže je další uchovávání výslovně nařízeno právním předpisem, v takovém případě se příslušné osobní údaje uchovávají a spravují odděleně od ostatních osobních údajů, nepoužijí se k žádnému jinému účelu, než který uvádí právní předpis, a na konci doby uchovávání se zničí;

3) zpracovává osobní údaje vhodným způsobem, který je nezbytný pro účely, pro které jsou osobní údaje zpracovávány, a tyto údaje nepoužívá nad rámec těchto účelů (čl. 3 odst. 2 zákona o ochraně osobních údajů);

4) zajišťuje, aby osobní údaje byly přesné, úplné a aktuální v míře nezbytné ve vztahu k účelům, pro které jsou tyto osobní údaje zpracovávány (čl. 3 odst. 3 zákona o ochraně osobních údajů);

5) zajišťuje bezpečnou správu osobních údajů podle metod zpracování, druhů osobních údajů atd., s přihlédnutím k možnosti porušení práv subjektu údajů a k závažnosti příslušných rizik (čl. 3 odst. 4 zákona o ochraně osobních údajů);

6) zveřejní své zásady ochrany soukromí a další záležitosti související se zpracováním osobních údajů (čl. 3 odst. 5 zákona o ochraně osobních údajů);

7) zpracovává osobní údaje způsobem, který minimalizuje možnost narušení soukromí subjektu údajů (čl. 3 odst. 6 zákona o ochraně osobních údajů).

ii) V souladu s čl. 58 odst. 4 zákona o ochraně osobních údajů správce (např. orgány příslušné v oblasti národní bezpečnosti, jako je Národní zpravodajská služba) přijme nezbytná opatření, například zavede technické, řídicí a fyzické záruky, aby zajistil dodržování těchto zásad a náležité zpracování osobních údajů. To může například zahrnovat zvláštní opatření k zajištění bezpečnosti osobních údajů, jako jsou omezení přístupu k osobním údajům, řízení přístupu, protokoly, specializovanou odbornou přípravu zaměstnanců zaměřenou na nakládání s osobními údaji atd.

Kromě toho mají v souladu s čl. 3 odst. 5 a článkem 4 zákona o ochraně osobních údajů subjekty údajů mimo jiné tato práva, pokud jde o osobní údaje zpracovávané pro účely národní bezpečnosti:

1) právo získat potvrzení o tom, zda osobní údaje subjektu údajů jsou či nejsou zpracovávány, jakož i informace o tomto zpracování a přístup k těmto údajům, včetně poskytnutí kopií (čl. 4 odst. 1 a 3 zákona o ochraně osobních údajů);

2) právo pozastavit zpracování a právo na opravu, výmaz a zničení osobních údajů (čl. 4 odst. 4 zákona o ochraně osobních údajů).

iii) Subjekt údajů může podat žádost o výkon těchto práv přímo správci nebo nepřímo prostřednictvím Komise pro ochranu osobních údajů a může k tomu zmocnit svého zástupce. Pokud subjekt údajů podá žádost, správce toto právo neprodleně udělí, přičemž však může toto právo pozdržet, omezit nebo odepřít, pokud je to výslovně stanoveno nebo je to nevyhnutelné pro dodržení jiných právních předpisů, a to na tak dlouho, jak je nezbytné a přiměřené k ochraně důležitého cíle veřejného zájmu (například v takovém rozsahu a po takovou dobu, kdy by udělení práva ohrozilo probíhající vyšetřování nebo národní bezpečnost), nebo pokud udělení práva může způsobit újmu na životě nebo zdraví třetí strany nebo neoprávněné narušení majetkových a jiných zájmů třetí strany. Pokud je žádost zamítnuta nebo omezena, správce neprodleně sdělí subjektu údajů příslušné důvody. Správce vypracuje metodu a postup, které subjektům údajů umožní podávat žádosti, a veřejně je oznámí, aby se o nich subjekty údajů mohly dozvědět.

Kromě toho v souladu s čl. 58 odst. 4 zákona o ochraně osobních údajů (požadavek na zajištění náležitého vyřízení individuálních stížností) a čl. 4 odst. 5 zákona o ochraně osobních údajů (právo na přiměřenou náhradu jakékoli škody vzniklé v důsledku zpracování osobních údajů, a to prostřednictvím rychlého a spravedlivého řízení) mají subjekty údajů právo na nápravu. To zahrnuje právo oznámit údajné porušení kontaktnímu centru pro oznamování případů porušení ochrany osobních údajů (v souladu s čl. 62 odst. 3 zákona o ochraně osobních údajů), podat podle článku 62 zákona o ochraně osobních údajů u Komise pro ochranu osobních údajů stížnost na jakékoli porušení práv nebo zájmů týkajících se osobních údajů jednotlivce a získat soudní ochranu proti rozhodnutím nebo nečinnosti Komise pro ochranu osobních údajů podle zákona o správním soudním řízení. Subjekty údajů mohou navíc získat soudní ochranu podle zákona o správním soudním řízení, pokud došlo k porušení jejich práv nebo zájmů z důvodu opatření nebo nečinnosti správce (např. nezákonné shromažďování osobních údajů), nebo získat náhradu škody v souladu se zákonem o náhradě škody státem. Tyto opravné prostředky jsou k dispozici jak v případě možného porušení pravidel obsažených ve zvláštních právních předpisech, kterými se stanoví omezení a záruky týkající se shromažďování osobních údajů, jako jsou právní předpisy v oblasti národní bezpečnosti, tak v případě možného porušení zákona o ochraně osobních údajů.

Fyzická osoba z EU může podat stížnost Komisi pro ochranu osobních údajů prostřednictvím svého vnitrostátního orgánu pro ochranu údajů a Komise pro ochranu osobních údajů bude tuto fyzickou osobu informovat prostřednictvím vnitrostátního orgánu pro ochranu údajů, jakmile je vyšetřování a případné nápravné opatření ukončeno.

PŘÍLOHA II

18. května 2021

Jeho Excelence Didier Reynders, komisař pro spravedlnost, Evropská komise

Vaše Excelence,

velice vítám konstruktivní jednání mezi Koreou a Evropskou komisí, jejichž cílem je vytvořit rámec pro předávání osobních údajů z EU do Koreje.

Na žádost Evropské komise, která byla určena korejské vládě, Vám v příloze zasílám dokument, který obsahuje přehled o právním rámci pro přístup korejské vlády k informacím.

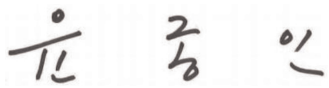
Tento dokument se týká mnoha ministerstev a vládních agentur Koreje a příslušná ministerstva a agentury (Komise pro ochranu osobních údajů, Ministerstvo spravedlnosti, Národní zpravodajská služba, Národní komise Koreje pro lidská práva, Národní centrum boje proti terorismu, Korejská finanční zpravodajská jednotka) v rámci svých příslušných pravomocí obsahově odpovídají za pasáže tohoto dokumentu. Níže naleznete příslušná ministerstva a agentury a odpovídající podpisy.

Komise pro ochranu osobních informací přijímá veškeré dotazy k tomuto dokumentu a bude koordinovat nezbytné odpovědi u příslušných ministerstev a agentur.

Doufám, že tento dokument bude pro rozhodování v Evropské komisi přínosný.

Děkujeme Vám za cenný příspěvek, který jste v této záležitosti dosud poskytli.

S úctou

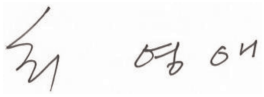


Yoon Jong In
předseda Komise pro ochranu osobních údajů

Tento dokument vypracovala Komise pro ochranu osobních údajů a níže uvedená ministerstva a agentury.

Park Jie Won
předseda (ředitel), Národní zpravodajská služba

Lee Jung Soo
generální ředitel, Ministerstvo spravedlnosti



Choi Young Ae
předsedkyně, Národní komise Koreje pro lidská práva

Kim Hyuck Soo
ředitel, Národní centrum boje proti terorismu

Kim Jeong Kag
komisař, Korejská finanční zpravodajská jednotka

Právní rámec pro shromažďování a používání osobních údajů korejskými orgány veřejné správy pro účely prosazování práva a národní bezpečnosti

Následující dokument poskytuje přehled o právním rámci pro shromažďování a používání osobních údajů korejskými orgány veřejné správy pro účely prosazování trestního práva a národní bezpečnosti (dále jen „*přístup vlády*“), zejména pokud jde o dostupné právní základy, platné podmínky (omezení) a záruky, včetně nezávislého dozoru a možností individuální ochrany.

1. OBECNÉ PRÁVNÍ ZÁSADY TÝKAJÍCÍ SE PŘÍSTUPU VLÁDY

1.1. Ústavní rámec

Ústava Korejské republiky stanoví právo na soukromí obecně (článek 17) a právo na soukromí korespondence konkrétně (článek 18). Je povinností státu, aby tato základní práva zajistil ([1]). Ústava dále stanoví, že práva a svobody občanů mohou být omezeny pouze zákonem, a vyžaduje-li to národní bezpečnost nebo zachování práva a pořádku pro veřejné blaho ([2]). Dokonce i pokud jsou taková omezení uložena, nesmí se dotknout podstaty svobody nebo práva ([3]). Korejské soudy uplatnily tato ustanovení v případech týkajících se zásahů vlády do soukromí. Nejvyšší soud například došel k závěru, že sledování civilistů porušuje základní právo na soukromí, přičemž zdůraznil, že občané mají „*právo na sebeurčení v oblasti osobních údajů*“ ([4]). V jiné věci Ústavní soud rozhodl, že soukromí je základním právem, které poskytuje ochranu před zásahy a sledováním ze strany státu v soukromém životě občanů ([5]).

Korejská ústava dále zaručuje, že žádná osoba nebude zatčena, zadržena, prohledána, vyslýchána, ani nebudou zajištěny žádné její věci, nestanoví-li tak zákon ([6]). Kromě toho lze prohlídky a zajištění věci provádět pouze na základě příkazu vydaného soudcem, na žádost státního zástupce a v souladu s řádným postupem ([7]). Za výjimečných okolností, tj. v případech, kdy je osoba podezřelá z trestného činu zadržena při páchání trestného činu (*flagrante delicto*) nebo kdy existuje riziko, že osoba podezřelá ze spáchání trestného činu, za který lze uložit trest odnětí svobody v délce nejméně tří let, může uprchnout nebo zničit důkazy, mohou vyšetřovací orgány provést prohlídku nebo zajištění věci bez soudního příkazu, o který musí v takovém případě požádat *ex post* ([8]). Tyto obecné zásady jsou dále rozpracovány ve zvláštních právních předpisech týkajících se trestního řízení a ochrany komunikace (podrobný přehled viz níže).

Pokud jde o cizí státní příslušníky, ústava stanoví, že jejich postavení je zaručeno podle mezinárodního práva a úmluv ([9]). Práva na ochranu soukromí zaručuje několik mezinárodních dohod, jichž je Korea smluvní stranou, například Mezinárodní pakt o občanských a politických právech (článek 17), Úmluva o právech osob se zdravotním postižením (článek 22) a Úmluva o právech dítěte (článek 16). Kromě toho, ačkoli ústava v zásadě zmiňuje práva „*občanů*“, Ústavní soud rozhodl, že i cizí státní příslušníci požívají základních práv ([10]). Soud zejména rozhodl, že ochrana důstojnosti a hodnoty člověka jako lidské bytosti, jakož i právo usilovat o štěstí jsou právy každé lidské bytosti, nikoli jen

([1]) Článek 10 ústavy Korejské republiky vyhlášené dne 17. července 1948 (dále jen „ústava“).
([2]) Ustanovení čl. 37 odst. 2 ústavy.
([3]) Ustanovení čl. 37 odst. 2 ústavy.
([4]) Rozhodnutí korejského Nejvyššího soudu 96DA42789, 24. července 1998.
([5]) Rozhodnutí Ústavního soudu 2002Hun-Ma51, 30. října 2003. Obdobně v rozhodnutích 99Hun-Ma513 a 2004Hun-Ma190 (spojené věci) ze dne 26. května 2005 Ústavní soud vysvětlil, že „*právo na kontrolu vlastních osobních údajů je právem subjektu údajů osobně rozhodnout, kdy, vůči komu nebo kým a do jaké míry budou jeho údaje zpřístupněny nebo použity. Jde o základní právo, které, jakkoli není upřesněno v ústavě, má chránit osobní svobodu rozhodování před rizikem způsobeným rozšířením funkcí státu a informačními a komunikačními technologiemi*.“
([6]) Ustanovení čl. 12 odst. 1 první věty ústavy.
([7]) Článek 16 a čl. 12 odst. 3 ústavy.
([8]) Ustanovení čl. 12 odst. 3 ústavy.
([9]) Ustanovení čl. 6 odst. 2 ústavy.
([10]) Rozhodnutí Ústavního soudu 93Hun-MA120, 29. prosince 1994. Viz také například rozhodnutí Ústavního soudu 2014Hun-Ma346 (31. května 2018), v němž soud shledal, že bylo porušeno ústavní právo na právního zástupce v případě súdánského státního příslušníka zadrženého na letišti. V jiné věci Ústavní soud konstatoval, že svoboda volby legálního pracoviště úzce souvisí s právem usilovat o štěstí, jakož i o lidskou důstojnost a hodnotu, a není tedy vyhrazena pouze občanům, ale může být zaručena i cizincům, kteří jsou v Korejské republice legálně zaměstnáni (rozhodnutí Ústavního soudu 2007Hun-Ma1083, 29. září 2011).

občanů ([11]). Soud rovněž objasnil, že právo na kontrolu osobních údajů je považováno za základní právo, které vychází z práva na důstojnost a usilování o štěstí a z práva na soukromý život ([12]). Ačkoli se judikatura dosud konkrétně nezabývala právem cizích státních příslušníků na soukromí, akademická obec obecně uznává, že články 12 až 22 ústavy (které zahrnují právo na soukromí i osobní svobodu) stanoví *„práva lidských bytostí“*.

A v neposlední řadě ústava stanoví i právo požadovat od orgánů veřejné správy spravedlivé odškodnění ([13]). Kromě toho na základě zákona o Ústavním soudu může kterákoli osoba, jejíž základní práva zaručená ústavou jsou porušena výkonem vládní moci (vyjma soudních rozsudků), podat ústavní stížnost Ústavnímu soudu ([14]).

1.2. **Obecná pravidla ochrany údajů**

Všeobecný právní předpis o ochraně údajů v Korejské republice, zákon o ochraně osobních údajů, se vztahuje na soukromý i veřejný sektor. Pokud jde o orgány veřejné správy, zákon o ochraně osobních údajů konkrétně uvádí povinnost formulovat zásady, které mají zabránit *„zneužívání a neoprávněnému užívání osobních údajů, indiskrétnímu dohledu a sledování atd. a posílit důstojnost lidských bytostí a soukromí jednotlivců“* ([15]).

Zpracování osobních údajů pro účely prosazování práva podléhá veškerým požadavkům zákona o ochraně osobních údajů. To například znamená, že orgány činné v trestním řízení musí dodržovat povinnosti týkající se zákonného zpracování, tj. opírat se o jeden z právních základů vyjmenovaných v zákoně o ochraně osobních údajů pro shromažďování, používání nebo poskytování osobních údajů (články 15 až 18 zákona o ochraně osobních údajů), jakož i o zásady účelového omezení (čl. 3 odst. 1 a 2 zákona o ochraně osobních údajů), přiměřenosti/minimalizace údajů (čl. 3 odst. 1 a 6 zákona o ochraně osobních údajů), omezeného uchovávání údajů (článek 21 zákona o ochraně osobních údajů), zabezpečení údajů včetně oznámení o porušení zabezpečení údajů (čl. 3 odst. 4, články 29 a 34 zákona o ochraně osobních údajů) a transparentnosti (čl. 3 odst. 1 a 5, články 20, 30 a 32 zákona o ochraně osobních údajů). Pokud jde o citlivé informace, platí zvláštní záruky (článek 23 zákona o ochraně osobních údajů). Kromě toho v souladu s čl. 3 odst. 5 a článkem 4 zákona o ochraně osobních údajů, jakož i s články 35 až 39-2 zákona o ochraně osobních údajů mohou jednotlivci vůči donucovacím orgánům uplatňovat svá práva na přístup, opravu, výmaz a pozastavení zpracování.

Zákon o ochraně osobních údajů se v plném rozsahu vztahuje na zpracování osobních údajů pro účely vymáhání trestního práva, obsahuje však výjimku pro případy, kdy jsou osobní údaje zpracovávány pro účely národní bezpečnosti. Podle čl. 58 odst. 1 bodu 2 zákona o ochraně osobních údajů se články 15 až 50 zákona o ochraně osobních údajů nepoužijí na osobní údaje shromážděné nebo požadované pro analýzu informací souvisejících s národní bezpečností ([16]). Pro zpracování takových osobních údajů zůstávají i nadále použitelné kapitola I (Všeobecná ustanovení), kapitola II (Stanovení zásad ochrany osobních údajů atd.), kapitola VIII (Hromadná žaloba týkající se porušení ochrany údajů), kapitola IX (Doplňková ustanovení) a kapitola X (Ustanovení o sankcích) zákona o ochraně osobních údajů. To zahrnuje obecné zásady ochrany údajů stanovené v článku 3 (Zásady ochrany osobních údajů) a individuální práva zaručená článkem 4 zákona o ochraně osobních údajů (Práva subjektů údajů). To znamená, že hlavní zásady a práva jsou zaručeny i v této oblasti. Kromě toho čl. 58 odst. 4 zákona o ochraně osobních údajů stanoví, že tyto údaje musí být zpracovávány v minimálním rozsahu nezbytném pro dosažení zamýšleného účelu a po minimální dobu, a požaduje také, aby správce osobních údajů zavedl nezbytná opatření k zajištění bezpečné správy údajů a náležitého zpracování, jako jsou technické, řídicí a fyzické záruky, jakož i opatření pro náležité vyřizování individuálních stížností.

V oznámení č. 2021-1 o doplňkových pravidlech pro výklad a použití zákona o ochraně osobních údajů Komise pro ochranu osobních údajů dále objasnila, jak se zákon o ochraně osobních údajů použije na zpracování osobních údajů pro účely národní bezpečnosti s ohledem na uvedenou dílčí výjimku ([17]). Zahrnuje to zejména práva fyzických osob (přístup, oprava, pozastavení zpracování a výmaz) a důvody, jakož i meze případných omezení těchto práv. Podle oznámení odráží uplatňování základních zásad, práv a povinností podle zákona o ochraně osobních údajů na

([11]) Rozhodnutí Ústavního soudu 99HeonMa494, 29. listopadu 2001.
([12]) Viz například rozhodnutí Ústavního soudu 99HunMa513.
([13]) Ustanovení čl. 29 odst. 1 ústavy.
([14]) Ustanovení čl. 68 odst. 1 zákona o Ústavním soudu.
([15]) Ustanovení čl. 5 odst. 1 zákona o ochraně osobních údajů.
([16]) Ustanovení čl. 58 odst. 1 bodu 2 zákona o ochraně osobních údajů.
([17]) Oznámení Komise pro ochranu osobních údajů č. 2021-1 o doplňkových pravidlech pro výklad a použití zákona o ochraně osobních údajů, oddíl III bod 6.

zpracování osobních údajů pro účely národní bezpečnosti záruky, které stanoví ústava na ochranu práva jednotlivce na kontrolu jeho osobních údajů. Jakékoli omezení tohoto práva, například je-li nezbytné pro ochranu národní bezpečnosti, vyžaduje vyvážení práv a zájmů jednotlivce vůči příslušnému veřejnému zájmu a nesmí se dotknout podstaty práva (čl. 37 odst. 2 ústavy).

2. PŘÍSTUP VLÁDY PRO ÚČELY PROSAZOVÁNÍ PRÁVA

2.1. Příslušné orgány veřejné správy v oblasti prosazování práva

Na základě zákona o trestním řízení, zákona o ochraně důvěrnosti komunikací a zákona o telekomunikačních službách mohou policie, státní zástupci a soudy shromažďovat osobní údaje pro účely prosazování trestního práva. V rozsahu, v němž zákon o Národní zpravodajské službě svěřuje tuto pravomoc také Národní zpravodajské službě, musí výše uvedené zákony dodržovat i Národní zpravodajská služba ([18]). A konečně zákon o oznamování a používání určitých informací o finančních transakcích stanoví právní základ pro finanční instituce, které zpřístupňují informace Korejské finanční zpravodajské jednotce pro účely prevence praní peněz a financování terorismu. Tato specializovaná agentura naopak může takové informace předávat donucovacím orgánům. Tyto povinnosti týkající se zpřístupnění se však vztahují pouze na správce údajů, kteří zpracovávají osobní úvěrové informace podle zákona o úvěrových informacích a podléhají dozoru Komise pro finanční služby. Vzhledem k tomu, že zpracování osobních úvěrových informací takovými správci je z oblasti působnosti rozhodnutí o odpovídající ochraně vyloučeno, nejsou v tomto dokumentu podrobněji popsána omezení a záruky platné v souladu se zákonem o oznamování a používání určitých informací o finančních transakcích.

2.2. Právní základy a omezení

Zákon o trestním řízení (viz 2.2.1), zákon o ochraně důvěrnosti komunikací (viz 2.2.2) a zákon o telekomunikacích (viz 2.2.3) poskytují právní základ pro shromažďování osobních údajů pro účely prosazování práva a stanoví příslušná omezení a záruky.

2.2.1. *Prohlídky a zajištění věci*

2.2.1.1. Právní základ

Státní zástupci a vyšší příslušníci soudní policie mohou provádět kontrolu předmětů, prohlídky osob nebo zajišťování věcí 1) pouze pokud je osoba podezřelá ze spáchání trestného činu (podezřelý z trestného činu); 2) je to nezbytné pro vyšetřování a 3) předměty, které mají být kontrolovány, osoby, které mají být prohledány, a jakékoli zajištěné věci jsou považovány za související s danou trestní věcí ([19]). Podobně mohou soudy provádět prohlídky a zajišťovat jakékoli věci, které mají být použity jako důkaz nebo mohou být zabaveny, pokud jsou takové věci nebo osoby považovány za související s konkrétní soudní věcí ([20]).

2.2.1.2. Omezení a záruky

Obecnou povinností státních zástupců a příslušníků soudní policie je respektovat lidská práva osob podezřelých z trestného činu i práva jakékoli jiné dotčené osoby ([21]). Kromě toho mohou být povinná opatření k dosažení účelu vyšetřování přijata pouze tehdy, jsou-li výslovně stanovena v zákoně o trestním řízení, a smí být přijata jen v nejmenším nezbytném rozsahu ([22]).

Pátrání, kontroly nebo zajištění věci prováděné policisty nebo státními zástupci v rámci vyšetřování trestné činnosti se mohou uskutečnit pouze na základě soudního příkazu ([23]). Orgán, který podává návrh na vydání příkazu, musí předložit materiály prokazující důvody podezření určité osoby ze spáchání trestného činu, nezbytnost prohlídky, kontroly nebo zajištění věci a existenci příslušných věcí, které mají být zajištěny ([24]). Soudní příkaz musí mimo jiných prvků uvádět jména osoby podezřelé z trestného činu a daný trestný čin; místo, osobu nebo věci, které mají být prohledány, nebo věci, které mají být zajištěny; datum vystavení a lhůtu platnosti příkazu ([25]). Obdobně platí, že pokud jsou v rámci probíhajícího soudního řízení prováděny prohlídky a zajištění věci jinak než na veřejném jednání, je třeba předem získat soudní příkaz ([26]). Dotčená osoba a její obhájce jsou o prohlídce nebo zajištění věci předem informováni a mohou být přítomni výkonu příkazu ([27]).

([18]) Viz článek 3 zákona o Národní zpravodajské službě (zákon č. 12948), který odkazuje na vyšetřování určitých trestných činů, jako jsou povstání, vzpoura a zločiny související s národní bezpečností (např. špionáž). V takovém kontextu by se použily postupy podle zákona o trestním řízení týkající se prohlídek a zajištění věci, zatímco zákonem o ochraně důvěrnosti komunikací by se řídilo shromažďování údajů o komunikaci (viz oddíl 3 o ustanoveních týkajících se přístupu ke komunikaci pro účely národní bezpečnosti).
([19]) Ustanovení čl. 215 odst. 1 a 2 zákona o trestním řízení.
([20]) Ustanovení čl. 106 odst. 1 a článků 107 a 109 zákona o trestním řízení.
([21]) Ustanovení čl. 198 odst. 2 zákona o trestním řízení.
([22]) Ustanovení čl. 199 odst. 1 zákona o trestním řízení.
([23]) Ustanovení čl. 215 odst. 1 a 2 zákona o trestním řízení.
([24]) Ustanovení čl. 108 odst. 1 trestního řádu.
([25]) Ustanovení čl. 114 odst. 1 zákona o trestním řízení ve spojení s článkem 219 zákona o trestním řízení.
([26]) Článek 113 zákona o trestním řízení.
([27]) Články 121 a 122 zákona o trestním řízení.

Při provádění prohlídek nebo zajištění věci a v případech, kde je předmětem prohlídky počítačový disk nebo jiné médium pro ukládání dat, budou zpravidla zajištěna pouze samotná data (zkopírovaná nebo vytištěná), nikoli celé médium ([28]). Samotné médium pro ukládání dat lze zajistit pouze za předpokladu, že je považováno za v podstatě nemožné vytisknout nebo zkopírovat požadovaná data samostatně, nebo pokud je považováno za v podstatě neproveditelné naplnit účel prohlídky jinak ([29]). Dotčená osoba musí být o zajištění věci neprodleně informována ([30]). Podle zákona o trestním řízení neexistují z tohoto požadavku na oznámení žádné výjimky.

Prohlídky, kontroly a zajištění věci bez soudního příkazu jsou přípustné pouze v omezených případech. Zaprvé, jde o případ, kdy soudní příkaz nelze získat z důvodu naléhavosti na místě činu ([31]). Soudní příkaz je však nutné neprodleně následně získat ([32]). Zadruhé, prohlídky a kontroly bez soudního příkazu se mohou konat na místě, pokud je osoba podezřelá z trestného činu zatčena nebo zadržena ([33]). A konečně může státní zástupce nebo vyšší příslušník soudní policie zajistit věc bez soudního příkazu, pokud se jí osoba podezřelá z trestného činu nebo třetí osoba zbavila nebo pokud byla věc vydána dobrovolně ([34]).

Důkazy získané v rozporu se zákonem o trestním řízení budou považovány za nepřípustné ([35]). Trestní zákon navíc stanoví, že za nezákonné prohlídky osob nebo místa bydliště osoby, střežené budovy, stavby, automobilu, lodi, letadla nebo obývaného prostoru lze uložit trest odnětí svobody v délce až tří let ([36]). Toto ustanovení se tedy vztahuje také na případy, kdy jsou věci, například zařízení pro ukládání dat, zajištěny během nezákonné prohlídky.

2.2.2. *Shromažďování údajů o komunikaci*

2.2.2.1. Právní základ

Shromažďování údajů o komunikaci je upraveno zvláštním zákonem, zákonem o ochraně důvěrnosti komunikací. Zákon o ochraně důvěrnosti komunikací stanoví zejména obecný zákaz cenzurovat jakoukoli poštu, odposlouchávat jakoukoli telekomunikaci, poskytovat údaje potvrzující komunikaci nebo zaznamenávat nebo poslouchat jakýkoli neveřejný hovor jiných osob, s výjimkou jednání na základě zákona o trestním řízení, zákona o ochraně důvěrnosti komunikací nebo zákona o vojenském soudu ([37]). Výraz „*komunikace*“ ve smyslu zákona o ochraně důvěrnosti komunikací zahrnuje běžnou poštu i telekomunikační sdělení ([38]). V tomto ohledu zákon o ochraně důvěrnosti komunikací rozlišuje mezi „*opatřeními omezujícími komunikaci*“ ([39]) a shromažďováním „*údajů potvrzujících komunikaci*“.

Výraz „opatření omezující komunikaci“ zahrnuje „*cenzuru*“, tj. shromažďování obsahu tradiční poštovní komunikace, jakož i „*odposlechy*“, tj. přímé odposlouchávání (získávání nebo zaznamenávání) obsahu telekomunikace ([40]). Pojem „údaje potvrzující komunikaci“ označuje „*údaje o záznamech telekomunikace*“, které zahrnují datum telekomunikace, čas zahájení a ukončení, počet odchozích a příchozích hovorů, stejně jako číslo druhého účastníka, četnost použití, protokoly o používání telekomunikačních služeb a informace o poloze (např. z přenosových věží, které přijímají signály) ([41]).

([28]) Ustanovení čl. 106 odst. 3 zákona o trestním řízení.
([29]) Ustanovení čl. 106 odst. 3 zákona o trestním řízení.
([30]) Článek 219 zákona o trestním řízení ve spojení s čl. 106 odst. 4 zákona o trestním řízení.
([31]) Ustanovení čl. 216 odst. 3 zákona o trestním řízení.
([32]) Ustanovení čl. 216 odst. 3 zákona o trestním řízení.
([33]) Ustanovení čl. 216 odst. 1 a 2 zákona o trestním řízení.
([34]) Článek 218 zákona o trestním řízení. Pokud jde o osobní údaje, vztahují se uvedená ustanovení pouze na jejich dobrovolné vydání dotyčnou osobou, nikoli správcem osobních údajů, který má takové údaje v držení (to by vyžadovalo zvláštní právní základ podle zákona o ochraně osobních údajů). Dobrovolně vydané věci jsou připuštěny jako důkaz v soudním řízení pouze za předpokladu, že neexistují rozumné pochybnosti o dobrovolnosti zpřístupnění, kterou musí prokázat státní zástupce. Viz rozhodnutí Nejvyššího soudu 2013Do11233 ze dne 10. března 2016.
([35]) Článek 308-2 zákona o trestním řízení.
([36]) Článek 321 trestního zákona.
([37]) Článek 3 zákon o ochraně důvěrnosti komunikací. Zákon o vojenském soudu v zásadě upravuje shromažďování údajů o příslušnících armády a na civilní osoby je použitelný pouze v omezeném počtu případů (např. pokud by příslušníci armády a civilní osoby spáchali trestný čin společně nebo pokud by se fyzická osoba dopustila trestného činu proti armádě, může být zahájeno řízení před vojenským soudem, viz článek 2 zákona o vojenském soudu). Obecná ustanovení upravující prohlídky a zajišťování věcí jsou obdobná jako v zákoně o trestním řízení, viz např. články 146 až 149 a 153 až 156 zákona o vojenském soudu. Například poštovní zásilky lze shromažďovat pouze tehdy, je-li to nutné pro vyšetřování, a to na základě příkazu vydaného vojenským soudem. Bude-li shromažďována elektronická komunikace, použijí se omezení a záruky podle zákona o ochraně důvěrnosti komunikací.
([38]) Ustanovení čl. 2 odst. 1 zákona o ochraně důvěrnosti komunikací, tj. „*přenos nebo příjem všech druhů zvuků, slov, symbolů nebo obrazového materiálu po drátě, bezdrátově, optickým kabelem nebo jiným elektromagnetickým systémem, včetně telefonu, e-mailu, informační služby vyžadující členství, faxu a pagingu*.“
([39]) Ustanovení čl. 2 odst. 7 čl. 3 odst. 2 zákona o ochraně důvěrnosti komunikací.
([40]) „Cenzura“ je definována jako „*otevírání pošty bez souhlasu dotčené strany nebo získávání poznatků, zaznamenávání nebo zadržování obsahu pošty jinými prostředky*“ (čl. 2 odst. 6 zákona o ochraně důvěrnosti komunikací). „Odposlechy“ se rozumí „*získávání nebo zaznamenávání obsahu telekomunikace poslechem nebo společným odečítáním zvuků, slov, symbolů nebo obrazového materiálu v rámci komunikace prostřednictvím elektronických a mechanických zařízení bez souhlasu dotčené strany nebo zasahování do jejich přenosu a příjmu*“ (čl. 2 odst. 7 zákona o ochraně důvěrnosti komunikací).
([41]) Ustanovení čl. 2 odst. 11 zákona o ochraně důvěrnosti komunikací.

Zákon o ochraně důvěrnosti komunikací stanoví omezení a záruky pro shromažďování obou druhů údajů a nedodržení některých z těchto požadavků podléhá trestním sankcím ([42]).

2.2.2.2. Omezení a záruky použitelné na shromažďování obsahu komunikace (opatření omezující komunikaci)

Shromažďování obsahu komunikace může probíhat pouze jako doplňkový prostředek usnadňující vyšetřování trestné činnosti (tj. jako opatření poslední instance) a je nutné vynaložit úsilí k minimalizaci zásahů do komunikačních tajemství lidí ([43]). V souladu s touto obecnou zásadou lze opatření omezující komunikaci uplatnit pouze v případě, že je obtížné jinak zabránit spáchání trestného činu, zatknout pachatele trestné činnosti nebo shromáždit důkazy ([44]). Donucovací orgány, které shromažďují obsah komunikace, musí tuto činnost okamžitě ukončit, jakmile již další přístup není považován za nezbytný, a zajistit tak, aby bylo narušování důvěrnosti komunikací omezeno co nejméně ([45]).

Opatření omezující komunikaci lze kromě toho použít pouze za předpokladu, že existuje závažný důvod k podezření, že jsou plánovány, páchány nebo spáchány některé závažné trestné činy konkrétně vyjmenované v zákoně o ochraně důvěrnosti komunikací. Tyto trestné činy zahrnují povstání, trestné činy související s drogami nebo trestné činy zahrnující výbušniny, jakož i trestné činy související s národní bezpečností, diplomatickými vztahy nebo vojenskými základnami a zařízeními ([46]). Cílem opatření omezujícího komunikaci musí být konkrétní poštovní zásilky nebo telekomunikační sdělení odeslané nebo přijaté podezřelou osobou nebo poštovní zásilky nebo telekomunikační sdělení odeslané nebo přijaté podezřelou osobou během pevně stanoveného časového období ([47]).

Dokonce i pokud jsou tyto požadavky splněny, může shromažďování údajů o obsahu probíhat pouze na základě soudního příkazu. Konkrétně může státní zástupce požádat soud o povolení shromažďování údajů o obsahu týkajících se podezřelé nebo vyšetřované osoby ([48]). Podobně může příslušník soudní policie požádat o povolení státního zástupce, který pak může předložit soudu návrh na vydání soudního příkazu ([49]). Návrh na vydání soudního příkazu musí být vyhotoven písemně a musí obsahovat konkrétní prvky. Zejména musí uvádět 1) podstatné důvody pro podezření, že je plánován, je páchán nebo byl spáchán jeden z vyjmenovaných trestných činů, jakož i veškeré materiály, které *prima facie* nasvědčují podezření; 2) opatření omezující komunikaci, jakož i jejich účel, rozsah, cíl a dobu účinnosti a 3) místo, kde by byla opatření provedena, a způsob, jakým by byla provedena ([50]).

Jsou-li splněny zákonné požadavky, může soud vydat písemné povolení k provedení opatření omezujících komunikaci ve vztahu k podezřelé nebo vyšetřované osobě ([51]). Tento soudní příkaz specifikuje druhy opatření a také jejich účel, rozsah, dobu účinnosti, místo provedení a způsob, jakým budou opatření prováděna ([52]).

Opatření omezující komunikaci lze provádět nejvýše po dobu dvou měsíců ([53]). Je-li cíle opatření dosaženo dříve v této lhůtě, musí být opatření okamžitě ukončena. Naopak pokud jsou požadované podmínky stále splněny, lze v dvouměsíční lhůtě podat žádost o prodloužení doby účinnosti opatření omezujících komunikaci. Taková žádost musí obsahovat materiály, které prima facie zakládají důvody k prodloužení opatření ([54]). Prodloužená lhůta nesmí celkově překročit jeden rok nebo tři roky v případě zvláště závažných trestných činů (např. trestných činů souvisejících s povstáním, zahraniční agresí, národní bezpečností atd.) ([55]).

Donucovací orgány si mohou vynutit součinnost poskytovatelů komunikačních služeb tak, že jim předloží písemný souhlas soudu ([56]). Poskytovatelé komunikačních služeb jsou povinni spolupracovat a uchovávat obdržené souhlasy ve své evidenci ([57]). Mohou součinnost odmítnout, pokud jsou údaje o cílové osobě uvedené v písemném souhlasu soudu (například telefonní číslo dané osoby) nesprávné. Kromě toho nesmí za žádných okolností zpřístupňovat hesla používaná pro telekomunikační služby ([58]).

([42]) Články 16 a 17 zákona o ochraně důvěrnosti komunikací. Týká se to například shromažďování údajů bez soudního příkazu, nevedení záznamů, neukončení shromažďování poté, co pomine mimořádná situace, nebo neposkytnutí oznámení dotčené osobě.
([43]) Ustanovení čl. 3 odst. 2 zákona o ochraně důvěrnosti komunikací.
([44]) Ustanovení čl. 5 odst. 1 zákona o ochraně důvěrnosti komunikací.
([45]) Článek 2 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([46]) Ustanovení čl. 5 odst. 1 zákona o ochraně důvěrnosti komunikací.
([47]) Ustanovení čl. 5 odst. 2 zákona o ochraně důvěrnosti komunikací.
([48]) Ustanovení čl. 6 odst. 1 zákona o ochraně důvěrnosti komunikací.
([49]) Ustanovení čl. 6 odst. 2 zákona o ochraně důvěrnosti komunikací.
([50]) Ustanovení čl. 6 odst. 4 zákona o ochraně důvěrnosti komunikací a čl. 4 odst. 1 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([51]) Ustanovení čl. 6 odst. 5 a 8 zákona o ochraně důvěrnosti komunikací.
([52]) Ustanovení čl. 6 odst. 6 zákona o ochraně důvěrnosti komunikací.
([53]) Ustanovení čl. 6 odst. 7 zákona o ochraně důvěrnosti komunikací.
([54]) Ustanovení čl. 6 odst. 7 zákona o ochraně důvěrnosti komunikací.
([55]) Ustanovení čl. 6 odst. 8 zákona o ochraně důvěrnosti komunikací.
([56]) Ustanovení čl. 9 odst. 2 zákona o ochraně důvěrnosti komunikací.
([57]) Ustanovení čl. 15-2 zákona o ochraně důvěrnosti komunikací a článku 12 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([58]) Ustanovení čl. 9 odst. 4 zákona o ochraně důvěrnosti komunikací.

Kdokoli, kdo provádí opatření omezující komunikaci nebo je požádán o součinnost, musí vést záznamy o cílech opatření, jejich provedení, datu poskytnutí součinnosti a o příslušném účelu ([59]). Také donucovací orgány, které provádějí opatření omezující komunikaci, musí vést záznamy uvádějící podrobnosti a dosažené výsledky ([60]). Příslušníci soudní policie musí tyto informace poskytnout ve zprávě státnímu zástupci při ukončení vyšetřování ([61]).

Pokud státní zástupce podá obžalobu týkající se případu, v němž byla použita opatření omezující komunikaci, nebo vydá rozhodnutí neobviňovat nebo nezadržovat příslušnou osobu (tj. nejen pokyn k zastavení trestního stíhání), musí státní zástupce danou osobu, vůči níž byla uplatněna opatření omezující komunikaci, informovat o tom, že byla tato opatření provedena, o agentuře, která je prováděla, a o době jejich provádění. Toto oznámení musí být poskytnuto písemně do 30 dnů od vydání rozhodnutí ([62]). Oznámení lze odložit, pokud je pravděpodobné, že by vážně ohrozilo národní bezpečnost nebo narušilo veřejnou bezpečnost a pořádek, nebo pokud by pravděpodobně způsobilo podstatnou újmu na životech a zdraví jiných osob ([63]). Pokud státní zástupce nebo příslušník soudní policie hodlá oznámení odložit, musí získat souhlas vedoucího představitele okresního státního zastupitelství ([64]). Jakmile důvody pro odklad pominou, musí být oznámení poskytnuto do 30 dnů od tohoto okamžiku ([65]).

Zákon o ochraně důvěrnosti komunikací také stanoví konkrétní postup pro shromažďování obsahu komunikací v mimořádných situacích. Donucovací orgány mohou zejména shromažďovat obsah komunikace v případě, že bezprostředně hrozí plánování nebo provedení organizované trestné činnosti nebo jiného závažného trestného činu, který může přímo způsobit smrt nebo vážnou újmu na zdraví, a nastane mimořádná situace, která znemožní uplatnit celý řádný postup (jak je uveden výše) ([66]). V takové mimořádné situaci může policista nebo státní zástupce přijmout opatření omezující komunikaci bez předchozího souhlasu soudu, musí však okamžitě po jeho provedení požádat o soudní souhlas. Pokud donucovací orgán nezíská povolení soudu do 36 hodin od okamžiku, kdy byla provedena mimořádná opatření, musí být shromažďování okamžitě zastaveno, přičemž obvykle následuje zničení shromážděných údajů ([67]). Policisté provádějící mimořádné sledování tak činí pod kontrolou státního zástupce nebo v případě, že nelze předem obdržet pokyny státního zástupce z důvodu nutnosti neprodleného jednání, musí policie získat souhlas státního zástupce ihned po zahájení opatření ([68]). Výše popsaná pravidla pro informování osob se použijí i pro shromažďování obsahu komunikace v mimořádných situacích.

Shromažďování údajů v mimořádných situacích musí vždy probíhat v souladu s „*prohlášením o mimořádné cenzuře/odposlechu*“ a orgán provádějící shromažďování musí vést registr všech mimořádných opatření ([69]). K žádosti o souhlas s mimořádnými opatřeními podané soudu musí být přiložen písemný dokument, v němž jsou uvedena nezbytná opatření omezující komunikaci, účel, předmět, rozsah, dobu, místo provedení, způsob a vysvětlení toho, jak příslušná opatření omezující komunikaci splňují čl. 5 odst. 1 zákona o ochraně důvěrnosti komunikací ([70]), spolu s podpůrnými dokumenty.

V případech, kdy jsou mimořádná opatření dokončena během krátké doby, a tudíž není vydáno soudní povolení (např. pokud je podezřelá osoba zatčena bezprostředně po zahájení odposlechu, který je proto ukončen), vedoucí příslušného státního zastupitelství podá příslušnému soudu oznámení o mimořádném opatření ([71]). V oznámení musí být uveden cíl, účel, rozsah, doba, místo provedení a způsob shromažďování údajů, jakož i důvody pro nepodání žádosti o souhlas soudu ([72]). Toto oznámení umožňuje přijímajícímu soudu přezkoumat zákonnost shromažďování údajů a musí být zapsáno do registru oznámení o mimořádných opatřeních.

([59]) Ustanovení čl. 9 odst. 3 zákona o ochraně důvěrnosti komunikací.
([60]) Ustanovení čl. 18 odst. 1 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([61]) Ustanovení čl. 18 odst. 2 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([62]) Ustanovení čl. 9-2 odst. 1 zákona o ochraně důvěrnosti komunikací.
([63]) Ustanovení čl. 9-2 odst. 4 zákona o ochraně důvěrnosti komunikací.
([64]) Ustanovení čl. 9-2 odst. 5 zákona o ochraně důvěrnosti komunikací.
([65]) Ustanovení čl. 9-2 odst. 6 zákona o ochraně důvěrnosti komunikací.
([66]) Ustanovení čl. 8 odst. 1 zákona o ochraně důvěrnosti komunikací.
([67]) Ustanovení čl. 8 odst. 2 zákona o ochraně důvěrnosti komunikací.
([68]) Ustanovení čl. 8 odst. 3 zákona o ochraně důvěrnosti komunikací a čl. 16 odst. 3 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([69]) Ustanovení čl. 8 odst. 4 zákona o ochraně důvěrnosti komunikací.
([70]) Tedy že existuje závažný důvod k podezření, že jsou plánovány nebo páchány nebo byly spáchány určité závažné trestné činy, a nelze jinak zabránit spáchání trestné činnosti, zatknout pachatele nebo shromáždit důkazy.
([71]) Ustanovení čl. 8 odst. 5 zákona o ochraně důvěrnosti komunikací.
([72]) Ustanovení čl. 8 odst. 6 a 7 zákona o ochraně důvěrnosti komunikací.

Obecným požadavkem je, že obsah komunikace získaný prostřednictvím opatření omezujících komunikaci na základě zákona o ochraně důvěrnosti komunikací lze použít pouze pro účely vyšetřování, trestního stíhání nebo prevence výše uvedených konkrétních trestných činů, v disciplinárním řízení pro tytéž trestné činy, pro účely nároku na náhradu škody podaného jednou ze stran komunikace nebo pokud to umožňují jiné zákony ([73]).

Při shromažďování telekomunikačních sdělení přenášených prostřednictvím internetu platí zvláštní záruky ([74]). Tyto údaje lze použít pouze k vyšetřování závažných trestných uvedených v čl. 5 odst. 1 zákona o ochraně důvěrnosti komunikací. Pro uchování údajů je třeba získat souhlas soudu, který schválil daná opatření omezující komunikaci ([75]). Žádost o uchování údajů musí obsahovat informace o opatřeních omezujících komunikaci, souhrn výsledků opatření, důvody uchovávání (spolu s podpůrnými materiály) a telekomunikační údaje, které mají být uchovány ([76]). Pokud taková žádost neexistuje, musí být získané telekomunikační údaje vymazány do 14 dnů po skončení opatření omezujících komunikaci ([77]). Pokud je žádost zamítnuta, musí být telekomunikační údaje zničeny do sedmi dnů ([78]). Pokud jsou telekomunikační údaje vymazány, musí být do sedmi dnů podána zpráva soudu, který schválil opatření omezující komunikaci, s uvedením důvodů výmazu, jakož i podrobností a harmonogramu výmazu.

Obecněji řečeno, pokud byly údaje nezákonně získány za pomoci opatření omezujících komunikaci, nebudou uznány jako důkaz v soudním nebo disciplinárním řízení ([79]). Zákon o ochraně důvěrnosti komunikací rovněž zakazuje jakékoli osobě, která přijímá opatření omezující komunikaci, zpřístupňovat důvěrné informace získané v průběhu provádění těchto opatření a používat získané informace k poškozování dobrého jména subjektů, na které se tato opatření vztahují ([80]).

2.2.2.3. Omezení a záruky použitelné na shromažďování údajů potvrzujících komunikaci

Podle zákona o ochraně důvěrnosti komunikací mohou donucovací orgány požádat poskytovatele telekomunikačních služeb o poskytnutí údajů potvrzujících komunikaci, je-li to nezbytné k provedení vyšetřování nebo výkonu trestu ([81]). Na rozdíl od shromažďování údajů o obsahu není možnost shromažďovat údaje potvrzující komunikaci omezena na určité konkrétní trestné činy. Stejně jako v případě údajů o obsahu však shromažďování údajů potvrzujících komunikaci vyžaduje předchozí písemný souhlas soudu, a to za stejných podmínek, jaké byly popsány výše ([82]). Pokud z důvodu naléhavosti nelze získat povolení soudu, mohou být údaje potvrzující komunikaci shromažďovány bez soudního příkazu; v takovém případě musí být souhlas získán bezprostředně po vyžádání údajů a musí být předán poskytovateli telekomunikačních služeb ([83]). Není-li získán následný souhlas, shromážděné údaje musí být zničeny ([84]).

Státní zástupci, příslušníci soudní policie a soudy musí vést evidenci žádostí o údaje potvrzující komunikaci ([85]). Kromě toho musí poskytovatelé telekomunikačních služeb dvakrát ročně podávat zprávu o zpřístupnění údajů potvrzujících komunikaci ministrovi pro vědu a IKT a musí uchovávat příslušné záznamy po dobu sedmi let ode dne zpřístupnění údajů ([86]).

Fyzickým osobám musí být zpravidla podáno oznámena skutečnost, že byly shromážděny údaje potvrzující komunikaci ([87]). Načasování takového oznámení závisí na okolnostech vyšetřování ([88]). Jakmile je přijato rozhodnutí zahájit/nezahájit trestní stíhání, musí být oznámení podáno do 30 dnů. Pokud je naopak obžaloba vzata zpět, musí být oznámení podáno do 30 dnů po uplynutí jednoho roku od přijetí tohoto rozhodnutí. V každém případě musí být oznámení podáno do 30 dnů po uplynutí jednoho roku od shromáždění údajů.

Oznámení lze odložit, pokud by mohlo 1) ohrozit národní bezpečnost, veřejnou bezpečnost a pořádek; 2) způsobit smrt nebo újmu na zdraví; 3) bránit spravedlivému soudnímu řízení (např. vést ke zničení důkazů nebo vyhrožování

([73]) Článek 12 zákon o ochraně důvěrnosti komunikací.
([74]) Článek 12-2 zákona o ochraně důvěrnosti komunikací.
([75]) Státní zástupce nebo policista, který provádí opatření omezující komunikaci, musí do 14 dnů po skončení opatření zvolit telekomunikační údaje, které mají být uchovány, a požádat o souhlas soudu (v případě návrhu policie musí být žádost podána státnímu zástupci, který následně předloží žádost soudu), viz čl. 12-2 odst. 1 a 2 zákona o ochraně důvěrnosti komunikací.
([76]) Ustanovení čl. 12-2 odst. 3 zákona o ochraně důvěrnosti komunikací.
([77]) Ustanovení čl. 12-2 odst. 5 zákona o ochraně důvěrnosti komunikací.
([78]) Ustanovení čl. 12-2 odst. 5 zákona o ochraně důvěrnosti komunikací.
([79]) Článek 4 zákon o ochraně důvěrnosti komunikací.
([80]) Ustanovení čl. 11 odst. 2 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([81]) Ustanovení čl. 13 odst. 1 zákona o ochraně důvěrnosti komunikací.
([82]) Články 13 a 6 zákona o ochraně důvěrnosti komunikací.
([83]) Ustanovení čl. 13 odst. 2 zákona o ochraně důvěrnosti komunikací. Stejně jako v případě naléhavých opatření omezujících komunikaci musí být vyhotoven dokument s podrobnostmi o případu (podezřelá osoba, opatření, která mají být přijata, trestný čin, na který existuje podezření, a naléhavost). Viz čl. 37 odst. 5 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([84]) Ustanovení čl. 13 odst. 3 zákona o ochraně důvěrnosti komunikací.
([85]) Ustanovení čl. 13 odst. 5 a 6 zákona o ochraně důvěrnosti komunikací.
([86]) Ustanovení čl. 13 odst. 7 zákona o ochraně důvěrnosti komunikací.
([87]) Viz čl. 13-3 odst. 7 ve spojení s článkem 9-2 zákona o ochraně důvěrnosti komunikací.
([88]) Ustanovení čl. 13-3 odst. 1 zákona o ochraně důvěrnosti komunikací.

svědkům) nebo 4) hanobit podezřelého, oběti nebo jiné osoby související s případem nebo narušit jejich soukromí ([89]). Oznámení týkající se jednoho z výše uvedených důvodů vyžaduje povolení ředitele příslušného okresního státního zastupitelství ([90]). Pokud důvody pro odklad pominou, musí být oznámení podáno do 30 dnů od tohoto okamžiku ([91]).

Osoby, které oznámení obdržely, mohou podat písemnou žádost státnímu zástupci nebo příslušníkovi soudní policie ohledně důvodů shromažďování údajů potvrzujících komunikaci ([92]). V takovém případě musí státní zástupce nebo příslušník soudní policie písemně uvést důvody do 30 dnů od obdržení žádosti, ledaže platí jeden z výše uvedených důvodů (výjimky odůvodňující odklad oznámení) ([93]).

2.2.3. *Dobrovolné zpřístupnění ze strany poskytovatelů telekomunikačních služeb*

Podle čl. 83 odst. 3 zákona o telekomunikačních službách mohou poskytovatelé telekomunikačních služeb dobrovolně vyhovět žádosti (podané na podporu soudního řízení v trestní věci, vyšetřování nebo výkonu trestu) soudu, státního zástupce nebo vedoucího vyšetřovací agentury o zpřístupnění „*komunikačních údajů*“. V kontextu zákona o telekomunikačních službách zahrnují „*komunikační údaje*“ jméno, registrační číslo rezidenta, adresu a telefonní číslo uživatelů, data, kdy se uživatelé přihlásí k odběru nebo ukončí předplatné, a také identifikační kódy uživatelů (tj. kódy používané k identifikaci oprávněného uživatele počítačových systémů nebo komunikačních sítí) ([94]). Pro účely zákona o telekomunikačních službách jsou za uživatele považováni pouze jednotlivci, kteří si objednávají služby přímo od korejského poskytovatele telekomunikačních služeb ([95]). V důsledku toho jsou situace, kdy by byly fyzické osoby z EU, jejichž údaje byly předány do Korejské republiky, považovány za uživatele podle zákona o telekomunikačních službách, pravděpodobně velmi omezené, protože tito jednotlivci neuzavírají přímou smlouvu s korejským poskytovatelem telekomunikačních služeb.

Žádosti o získání komunikačních údajů na základě zákona o telekomunikačních službách musí být podány písemně a musí obsahovat důvody žádosti, odkaz na příslušného uživatele a rozsah požadovaných údajů ([96]). Není-li možné z důvodu naléhavosti podat písemnou žádost, musí být písemná žádost podána, jakmile pomine důvod této naléhavosti ([97]). Poskytovatelé telekomunikačních služeb, kteří vyhoví žádostem o zpřístupnění komunikačních údajů, musí uchovávat složky obsahující záznamy o tom, že byly poskytnuty komunikační údaje, jakož i související materiály, například písemnou žádost ([98]). Kromě toho musí poskytovatelé telekomunikačních služeb dvakrát ročně podávat zprávy o poskytování komunikačních údajů ministrovi pro vědu a IKT ([99]).

Poskytovatelé telekomunikačních služeb nemají povinnost vyhovět žádostem o zpřístupnění komunikačních údajů na základě zákona o telekomunikačních službách. Každou žádost proto musí poskytovatel posoudit s ohledem na příslušné požadavky týkající se ochrany údajů podle zákona o ochraně osobních údajů. Poskytovatel telekomunikačních služeb musí zejména vzít v úvahu zájmy subjektu údajů a nesmí tyto informace zpřístupnit, pokud by to mohlo nekorektním způsobem narušit zájem jednotlivce nebo třetí strany ([100]). Kromě toho musí být v souladu s oznámením č. 2021-1 o doplňkových pravidlech pro výklad a použití zákona o ochraně osobních údajů o zpřístupnění údajů informována dotčená osoba. Ve výjimečných situacích může být takové oznámení odloženo, zejména pokud a dokud by ohrozilo probíhající vyšetřování trestného činu nebo by pravděpodobně způsobilo újmu na životě či zdraví jiné osoby, přičemž tato práva nebo tyto zájmy jsou zjevně nadřazeny právům subjektu údajů ([101]).

V roce 2016 Nejvyšší soud potvrdil, že dobrovolné poskytování komunikačních dat poskytovateli telekomunikačních služeb bez soudního příkazu na základě zákona o telekomunikačních službách jako takové neporušuje právo na informační sebeurčení uživatele telekomunikační služby. Současně soud objasnil, že k takovému porušení by došlo, pokud by bylo zjevně zřejmé, že dožadující orgán zneužil svého oprávnění požadovat zpřístupnění údajů o komunikaci, a tím porušil zájmy dotčené fyzické osoby nebo třetí strany ([102]). Obecněji řečeno, každá žádost o dobrovolné zpřístupnění podaná donucovacím orgánem musí být v souladu se zásadami zákonnosti, nezbytnosti a proporcionality vyplývajícími z korejské ústavy (čl. 12 odst. 1 a čl. 37 odst. 2).

([89]) Ustanovení čl. 13-3 odst. 2 zákona o ochraně důvěrnosti komunikací.
([90]) Ustanovení čl. 13-3 odst. 3 zákona o ochraně důvěrnosti komunikací.
([91]) Ustanovení čl. 13-3 odst. 4 zákona o ochraně důvěrnosti komunikací.
([92]) Ustanovení čl. 13-3 odst. 5 zákona o ochraně důvěrnosti komunikací.
([93]) Ustanovení čl. 13-3 odst. 6 zákona o ochraně důvěrnosti komunikací.
([94]) Ustanovení čl. 83 odst. 3 zákona o telekomunikačních službách.
([95]) Ustanovení čl. 2 odst. 9 zákona o telekomunikačních službách.
([96]) Ustanovení čl. 83 odst. 4 zákona o telekomunikačních službách.
([97]) Ustanovení čl. 83 odst. 4 zákona o telekomunikačních službách.
([98]) Ustanovení čl. 83 odst. 5 zákona o telekomunikačních službách.
([99]) Ustanovení čl. 83 odst. 6 zákona o telekomunikačních službách.
([100]) Ustanovení čl. 18 odst. 2 zákona o ochraně osobních údajů.
([101]) Oznámení Komise pro ochranu osobních údajů č. 2021-1 o doplňkových pravidlech pro výklad a použití zákona o ochraně osobních údajů, oddíl III bod 2 podbod iii).
([102]) Rozhodnutí Nejvyššího soudu 2012Da105482, 10. března 2016.

2.3. **Dozor**

Dohled nad donucovacími orgány se provádí pomocí různých mechanismů a zajišťují jej interní i externí subjekty.

2.3.1. *Vlastní audit*

V souladu se zákonem o auditech ve veřejném sektoru se orgánům veřejné správy doporučuje zřídit interní orgán pro vlastní audit, jehož úkolem je mimo jiné provádět kontrolu zákonnosti ([103]). Vedoucím představitelům těchto auditních subjektů musí být v největší možné míře zaručena nezávislost ([104]). Konkrétně jsou jmenováni z řad osob mimo příslušný orgán (např. bývalí soudci, profesoři) na období dvou až pěti let a mohou být odvoláni pouze z oprávněných důvodů (např. nejsou schopni vykonávat funkci z důvodu duševní nebo tělesné poruchy, je jim uloženo disciplinární opatření) ([105]). Auditoři jsou rovněž jmenováni na základě konkrétních podmínek stanovených zákonem ([106]). Zprávy o auditu mohou obsahovat doporučení nebo žádosti o kompenzaci nebo nápravu, jakož i napomenutí a doporučení nebo žádosti o disciplinární opatření ([107]). Vedoucí představitel orgánu veřejné správy, který je předmětem auditu, jakož i Rada pro audit a inspekce (viz oddíl 2.3.2) jsou o zprávách informováni do 60 dnů od dokončení auditu ([108]). Dotčený orgán musí provést požadovaná opatření a oznámit výsledky Radě pro audit a inspekce ([109]). Výsledky auditu jsou navíc obvykle dostupné široké veřejnosti ([110]). Odmítnutí nebo maření vlastního auditu podléhá správním pokutám ([111]). V oblasti vymáhání trestního práva Národní policejní agentura za účelem zajištění souladu s výše uvedenými právními předpisy využívá systém generálních inspektorů, který zajišťuje interní audity, a to i s ohledem na možné porušování lidských práv ([112]).

2.3.2. *Rada pro audit a inspekce*

Rada pro audit a inspekce může kontrolovat činnost orgánů veřejné správy a na základě těchto inspekcí vydávat doporučení, požadovat disciplinární opatření nebo podat trestní oznámení ([113]). Rada pro audit a inspekce je podřízena prezidentovi Korejské republiky, zachovává si však nezávislé postavení, pokud jde o její povinnosti ([114]). Kromě toho zákon o zřízení Rady pro audit a inspekce požaduje, aby byla Radě pro audit a inspekce poskytnuta maximální nezávislost, pokud jde o jmenování, propouštění a organizaci jejích zaměstnanců, jakož i sestavování rozpočtu ([115]). Předsedu Rady pro audit a inspekce jmenuje prezident se souhlasem Národního shromáždění ([116]). Šest zbývajících komisařů jmenuje prezident na doporučení předsedy, a to na čtyřleté funkční období ([117]). Komisaři (včetně předsedy) musí splňovat specifické požadavky na způsobilost stanovené zákonem ([118]) a mohou být odvoláni pouze v případě obžaloby, odsouzení k trestu odnětí svobody nebo neschopnosti plnit své povinnosti z důvodu dlouhodobé duševní nebo fyzické nezpůsobilosti ([119]). Komisaři mají navíc zakázáno účastnit se politických činností a souběžně zastávat funkce v Národním shromáždění, správních úřadech, organizacích podléhajících auditu a inspekci Rady pro audit a inspekce nebo jakýkoli jiný placený úřad nebo funkci ([120]).

Rada pro audit a inspekce provádí roční obecný audit, může však také provádět konkrétní audity v záležitostech zvláštního zájmu. Rada pro audit a inspekce si může v průběhu inspekce vyžádat předložení dokladů a požádat o účast jednotlivých osob ([121]). V rámci auditu Rada pro audit a inspekce zkoumá příjmy a výdaje státu, ale také dohlíží

([103]) Články 3 a 5 zákona o auditech ve veřejném sektoru.
([104]) Článek 7 zákona o auditech ve veřejném sektoru.
([105]) Články 8 až 11 zákona o auditech ve veřejném sektoru.
([106]) Článek 16 a násl. zákona o auditech ve veřejném sektoru.
([107]) Ustanovení čl. 23 odst. 2 zákona o auditech ve veřejném sektoru.
([108]) Ustanovení čl. 23 odst. 1 zákona o auditech ve veřejném sektoru.
([109]) Ustanovení čl. 23 odst. 3 zákona o auditech ve veřejném sektoru.
([110]) Článek 26 zákona o auditech ve veřejném sektoru.
([111]) Článek 41 zákona o auditech ve veřejném sektoru.
([112]) Viz zejména divize podřízené generálnímu řediteli pro audit a inspekce: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Články 24 a 31 až 35 zákona o Radě pro audit a inspekce.
([114]) Ustanovení čl. 2 odst. 1 zákona o Radě pro audit a inspekce.
([115]) Ustanovení čl. 2 odst. 2 zákona o Radě pro audit a inspekce.
([116]) Ustanovení čl. 4 odst. 1 zákona o Radě pro audit a inspekce.
([117]) Ustanovení čl. 5 odst. 1 a článku 6 zákona o Radě pro audit a inspekce.
([118]) Např. výkon činnosti soudce, státního zástupce nebo advokáta po dobu nejméně deseti let, státního úředníka nebo profesora nebo vyšší funkce na univerzitě po dobu nejméně osmi let nebo nejméně deset let práce ve společnosti kotované na burze nebo v instituci s vládními investicemi (z toho nejméně pět let jako výkonný ředitel), viz článek 7 zákona o Radě pro audit a inspekce.
([119]) Článek 8 zákona o Radě pro audit a inspekce.
([120]) Článek 9 zákona o Radě pro audit a inspekce.
([121]) Viz např. článek 27 zákona o Radě pro audit a inspekce.

na obecné dodržování povinností orgánů veřejné správy a veřejných činitelů s cílem zlepšit fungování veřejné správy ([122]). Její dozor proto přesahuje rozpočtové aspekty a zahrnuje i kontrolu zákonnosti.

2.3.3. *Národní shromáždění*

Národní shromáždění může vyšetřovat orgány veřejné správy a provádět jejich inspekce ([123]). Během vyšetřování nebo inspekce může Národní shromáždění požádat o zpřístupnění dokumentů a vynutit si účast svědků ([124]). Na každého, kdo se během vyšetřování Národního shromáždění dopustí křivé přísahy, se vztahují trestní sankce (odnětí svobody až na deset let) ([125]). Průběh a výsledky inspekcí mohou být zveřejněny ([126]). Pokud Národní shromáždění zjistí nezákonnou nebo nevhodnou činnost, může požádat, aby příslušný orgán veřejné správy přijal nápravná opatření, včetně přiznání odškodného, přijetí disciplinárních opatření a zlepšení vnitřních postupů ([127]). Na základě takové žádosti musí orgán neprodleně jednat a oznámit výsledek Národnímu shromáždění ([128]).

2.3.4. *Komise pro ochranu osobních údajů*

Komise pro ochranu osobních údajů vykonává dozor nad zpracováním osobních údajů donucovacími orgány v souladu se zákonem o ochraně osobních údajů. Kromě toho se podle čl. 7-8 odst. 3 a 4 a čl. 7-9 odst. 5 zákona o ochraně osobních údajů dozor Komise pro ochranu osobních údajů vztahuje rovněž na možná porušení pravidel, která stanoví omezení a záruky týkající se shromažďování osobních údajů, včetně pravidel obsažených ve zvláštních zákonech upravujících shromažďování (elektronických) důkazů pro účely vymáhání trestního práva (viz oddíl 2.2). Vzhledem k požadavkům čl. 3 odst. 1 zákona o ochraně osobních údajů na zákonné a korektní shromažďování osobních údajů představuje každé takové porušení také porušení zákona o ochraně osobních údajů, což Komisi pro ochranu osobních údajů umožňuje provádět vyšetřování a přijímat nápravná opatření ([129]).

Při výkonu dozorové funkce má Komise pro ochranu osobních údajů přístup ke všem relevantním informacím ([130]). Komise pro ochranu osobních údajů může poskytovat donucovacím orgánům rady ke zlepšení úrovně ochrany osobních údajů při jejich zpracovávání, ukládat nápravná opatření (např. pozastavit zpracování údajů nebo přijmout nezbytná opatření k ochraně osobních údajů) nebo doporučit orgánu, aby přijal disciplinární opatření ([131]). A konečně se předpokládají trestní sankce za určitá porušení zákona o ochraně osobních údajů, jako je nezákonné používání nebo zpřístupňování osobních údajů třetím stranám nebo nezákonné zpracování citlivých údajů ([132]). V tomto ohledu může Komise pro ochranu osobních údajů věc postoupit příslušnému vyšetřovacímu orgánu (včetně státního zástupce) ([133]).

2.3.5. *Národní komise pro lidská práva*

Národní komise pro lidská práva (nezávislý orgán pověřený ochranou a prosazováním základních práv) ([134]) má pravomoc vyšetřovat a napravovat porušování článků 10 až 22 ústavy, které zahrnují právo na soukromí a právo na soukromí korespondence. Národní komise pro lidská práva se skládá z jedenácti komisařů, kteří jsou na základě návrhu jmenováni Národním shromážděním (čtyři komisaři), prezidentem (čtyři komisaři) a předsedou Nejvyššího soudu (tři komisaři) ([135]). Aby mohl být jmenován, musí komisař 1) působit alespoň deset let na univerzitě nebo v autorizovaném výzkumném ústavu, a to alespoň jako docent; 2) působit jako soudce, státní zástupce nebo advokát po dobu nejméně deseti let; 3) vykonávat činnosti v oblasti lidských práv po dobu nejméně deseti let (např. pro neziskovou, nevládní organizaci nebo mezinárodní organizaci) nebo 4) být doporučen skupinami občanské společnosti ([136]). Předsedu jmenuje prezident z řad komisařů a musí jej potvrdit Národní

([122]) Články 20 a 24 zákona o Radě pro audit a inspekce.
([123]) Článek 128 zákona o Národním shromáždění a články 2, 3 a 15 zákona o inspekci a vyšetřování ve státní správě. To zahrnuje každoroční inspekce záležitostí státní správy jako celku a vyšetřování konkrétních záležitostí.
([124]) Ustanovení čl. 10 odst. 1 zákona o inspekci a vyšetřování ve státní správě. Viz rovněž články 128 a 129 zákona o Národním shromáždění.
([125]) Článek 14 zákona o svědectví, oceňování atd. před Národním shromážděním.
([126]) Ustanovení čl. 12-2 zákona o inspekci a vyšetřování ve státní správě.
([127]) Ustanovení čl. 16 odst. 2 zákona o inspekci a vyšetřování ve státní správě.
([128]) Ustanovení čl. 16 odst. 3 zákona o inspekci a vyšetřování ve státní správě.
([129]) Viz Oznámení Komise pro ochranu osobních údajů č. 2021-1 o doplňkových pravidlech pro výklad a použití zákona o ochraně osobních údajů.
([130]) Článek 63 zákona o ochraně osobních údajů.
([131]) Ustanovení čl. 61 odst. 2, čl. 65 odst. 1 a 2 a čl. 64 odst. 4 zákona o ochraně osobních údajů.
([132]) Ustanovení článků 70 až 74 zákona o ochraně osobních údajů.
([133]) Ustanovení čl. 65 odst. 1 zákona o ochraně osobních údajů.
([134]) Článek 1 zákona o Národní komisi pro lidská práva.
([135]) Ustanovení čl. 5 odst. 1 a 2 zákona o Národní komisi pro lidská práva.
([136]) Ustanovení čl. 5 odst. 3 zákona o Národní komisi pro lidská práva.

shromáždění ([137]). Komisaři (včetně předsedy) jsou jmenováni na tříleté funkční období, které lze prodloužit, a mohou být odvoláni pouze v případě, že jsou odsouzeni k trestu odnětí svobody nebo již nejsou schopni plnit své úkoly z důvodu dlouhodobé fyzické nebo duševní nezpůsobilosti (v takovém případě musí s odvoláním souhlasit dvě třetiny komisařů) ([138]). Členové Národní komise pro lidská práva mají zakázáno vykonávat souběžnou funkci v Národním shromáždění, místních radách nebo v orgánu celostátní nebo místní správy (jako úřední osoba) ([139]).

Národní komise pro lidská práva může zahájit vyšetřování z vlastního podnětu, nebo na žádost jednotlivce. V rámci svého vyšetřování může Národní komise pro lidská práva požádat o předložení příslušných materiálů, provádět inspekce a předvolávat fyzické osoby k podání výpovědi ([140]). V návaznosti na vyšetřování může Národní komise pro lidská práva vydat doporučení ke zlepšení nebo opravě konkrétních zásad a postupů a může je zveřejnit ([141]). Orgány veřejné správy musí Národní komisi pro lidská práva oznámit plán provádění takových doporučení do 90 dnů od jejich obdržení ([142]). Kromě toho v případě, že doporučení nejsou provedena, musí o tom dotčený orgán vyrozumět Komisi ([143]). Národní komise pro lidská práva může následně takové neplnění oznámit Národnímu shromáždění a/nebo zveřejnit. Orgány veřejné správy obecně dodržují doporučení Národní komise pro lidská práva a mají k tomu silnou motivaci, neboť jejich provádění bylo posouzeno jako součást obecného hodnocení, které provádí Úřad pro koordinaci vládní politiky pod vedením úřadu předsedy vlády.

2.4. **Individuální ochrana**

2.4.1. *Ochranné mechanismy dostupné podle zákona o ochraně osobních údajů*

Pokud jde o osobní údaje zpracovávané donucovacími orgány, mohou jednotlivci vykonávat svá práva na přístup, opravu, výmaz a pozastavení zpracování podle zákona o ochraně osobních údajů. O přístup lze požádat přímo u příslušného orgánu nebo nepřímo prostřednictvím Komise pro ochranu osobních údajů ([144]). Příslušný orgán může přístup omezit nebo odepřít pouze tehdy, je-li to stanoveno zákonem, pokud by to pravděpodobně způsobilo újmu na životě nebo zdraví třetí strany nebo by to pravděpodobně vedlo k neoprávněnému narušení majetkových a jiných zájmů jiné osoby (tj. pokud by zájmy jiné osoby převažovaly nad zájmy jednotlivce, který žádost podal) ([145]). Pokud je žádost o přístup zamítnuta, musí být jednotlivec informován o důvodech zamítnutí a způsobu podání opravného prostředku ([146]). Podobně může být žádost o opravu nebo výmaz zamítnuta, pokud to stanoví jiné právní předpisy, přičemž v takovém případě musí být osoba informována o souvisejících důvodech a možnosti podat opravný prostředek ([147]).

Pokud jde o opravné prostředky, může fyzická osoba podat stížnost Komisi pro ochranu osobních údajů prostřednictvím kontaktního centra pro ochranu soukromí, které provozuje Korejská agentura pro internet a zabezpečení ([148]). Kromě toho může mediační výbor pro spory týkající se osobních údajů zajistit fyzické osobě mediaci ([149]). Tyto opravné prostředky jsou k dispozici v případě možného porušení pravidel obsažených ve zvláštních právních předpisech, kterými se stanoví omezení a záruky týkající se shromažďování osobních údajů (oddíl 2.2), i v případě možného porušení zákona o ochraně osobních údajů. Kromě toho mohou fyzické osoby napadnout rozhodnutí nebo nečinnost Komise pro ochranu osobních údajů podle zákona o správním soudním řízení (viz oddíl 2.4.3).

([137]) Ustanovení čl. 5 odst. 5 zákona o Národní komisi pro lidská práva.
([138]) Ustanovení čl. 7 odst. 1 a článku 8 zákona o Národní komisi pro lidská práva.
([139]) Článek 10 zákona o Národní komisi pro lidská práva.
([140]) Článek 36 zákona o Národní komisi pro lidská práva. V souladu s čl. 36 odst. 7 zákona může být předložení materiálů nebo věcí odmítnuto, pokud by ohrozilo utajení ze strany státu, které by mohlo mít podstatný vliv na bezpečnost státu nebo diplomatické vztahy, nebo by představovalo závažnou překážku pro vyšetřování trestné činnosti nebo probíhající soudní řízení. V takových případech si může Komise podle potřeby vyžádat od vedoucího představitele příslušné agentury (který musí v dobré víře vyhovět) další informace, je-li to nezbytné ke kontrole toho, zda je odmítnutí poskytnout údaje odůvodněné.
([141]) Ustanovení čl. 25 odst. 1 zákona o Národní komisi pro lidská práva.
([142]) Ustanovení čl. 25 odst. 3 zákona o Národní komisi pro lidská práva.
([143]) Ustanovení čl. 25 odst. 4 zákona o Národní komisi pro lidská práva.
([144]) Ustanovení čl. 35 odst. 2 zákona o ochraně osobních údajů.
([145]) Ustanovení čl. 35 odst. 4 zákona o ochraně osobních údajů.
([146]) Ustanovení čl. 42 odst. 2 prováděcí vyhlášky k zákonu o ochraně osobních údajů.
([147]) Ustanovení čl. 36 odst. 1 a 2 zákona o ochraně osobních údajů a čl. 43 odst. 3 prováděcí vyhlášky k zákonu o ochraně osobních údajů.
([148]) Článek 62 zákona o ochraně osobních údajů.
([149]) Články 40 až 50 zákona o ochraně osobních údajů a články 48-2 až 57 prováděcí vyhlášky k zákonu o ochraně osobních údajů.

2.4.2. *Opravné prostředky u Národní komise pro lidská práva*

Národní komise pro lidská práva vyřizuje stížnosti fyzických osob (korejských i cizích státních příslušníků) na porušování lidských práv ze strany orgánů veřejné správy ([150]). Pro podání stížnosti Národní komisi pro lidská práva fyzickou osobou není stanoven žádný pevný požadavek ([151]). Národní komise pro lidská práva se proto bude stížností zabývat, i pokud dotčená osoba nemůže ve fázi posouzení přípustnosti prokázat újmu. V souvislosti se shromažďováním osobních údajů pro účely vymáhání trestního práva by proto fyzická osoba k tomu, aby byla stížnost Národní komisi pro lidská práva přípustná, nemusela prokazovat, že korejské orgány veřejné správy skutečně získaly přístup k jejím osobním údajům. Fyzická osoba může také požádat o řešení stížnosti prostřednictvím mediace ([152]).

K prošetření stížnosti může Národní komise pro lidská práva využít svých vyšetřovacích pravomocí, včetně žádosti o předložení příslušných materiálů, provedení inspekcí a předvolání jednotlivců k podání výpovědi ([153]). Pokud vyšetřování odhalí, že došlo k porušení příslušných právních předpisů, může Národní komise pro lidská práva doporučit provedení nápravných opatření nebo nápravu či zlepšení jakéhokoli příslušného právního předpisu, instituce, politiky nebo postupu ([154]). Navrhovaná náprava může zahrnovat mediaci, ukončení porušování lidských práv, náhradu škody a opatření, která zamezí opakování téhož nebo podobného porušování práv ([155]). V případě protiprávního shromažďování osobních údajů podle použitelných pravidel mohou nápravná opatření zahrnovat výmaz shromážděných osobních údajů. Pokud se považuje za vysoce pravděpodobné, že porušování práv nadále pokračuje, a v případě, že by toto porušování nebylo řešeno, a tím by způsobilo obtížně napravitelnou škodu, může Národní komise pro lidská práva přijmout naléhavá nápravná opatření ([156]).

Ačkoli Národní komise pro lidská práva nemá donucovací pravomoc, její rozhodnutí (např. rozhodnutí nepokračovat ve vyšetřování stížnosti) ([157]) a doporučení lze napadnout u korejských soudů podle zákona o správním soudním řízení (viz oddíl 2.4.3 níže) ([158]). Pokud navíc zjištění Národní komise pro lidská práva odhalí, že orgán veřejné správy shromažďoval osobní údaje nezákonně, mohla by se fyzická osoba vůči tomuto orgánu domáhat další nápravy u korejských soudů, např. napadením shromažďování údajů podle zákona o správním soudním řízení, podáním ústavní stížnosti podle zákona o Ústavním soudu nebo podáním žádosti o odškodnění podle zákona o náhradě škody státem (viz oddíl 2.4.3 níže).

2.4.3. *Soudní ochrana*

Fyzické osoby se mohou omezení a záruk popsaných v předchozích oddílech pro dosažení nápravy u korejských soudů dovolávat různými způsoby.

Zaprvé mohou být podle zákona o trestním řízení dotčená osoba a její právní zástupce přítomni výkonu příkazu k prohlídce nebo zajištění věci, a proto mohou vznést námitku v době výkonu příkazu ([159]). Kromě toho zákon o trestním řízení stanoví tzv. mechanismus „kvazistížností“, který jednotlivcům umožňuje obrátit se na příslušný soud se žádostí o zrušení nebo změnu opatření státního zástupce nebo policisty týkajícího se zajištění věci ([160]). To fyzickým osobám umožňuje napadnout opatření přijatá k výkonu příkazu týkajícího se zajištění věci.

([150]) Ačkoli článek 4 zákona o Národní komisi pro lidská práva uvádí občany a cizí státní příslušníky s bydlištěm v Korejské republice, výraz „s bydlištěm“ odráží spíše koncept soudní příslušnosti než koncept území. Pokud tedy vnitrostátní instituce v Koreji poruší základní práva cizího státního příslušníka, může tato osoba podat stížnost Národní komisi pro lidská práva. Viz například příslušná otázka na stránce Komise pro lidská práva věnované často kladeným otázkám, k dispozici na adrese https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Tak by tomu bylo v případě, že by k osobním údajům cizího státního příslušníka předaným do Koreje získaly nezákonný přístup korejské orgány veřejné správy.

([151]) Stížnost musí být zpravidla podána do jednoho roku od porušení práv, Národní komise pro lidská práva se však může přesto rozhodnout prošetřit stížnost podanou po této lhůtě, pokud neuplynula promlčecí lhůta podle trestního nebo občanského práva (čl. 32 odst. 1 bod 4 zákona o Národní komisi pro lidská práva).

([152]) Článek 42 a násl. zákona o Národní komisi pro lidská práva.

([153]) Články 36 a 37 zákona o Národní komisi pro lidská práva.

([154]) Článek 44 zákona o Národní komisi pro lidská práva.

([155]) Ustanovení čl. 42 odst. 4 zákona o Národní komisi pro lidská práva.

([156]) Článek 48 zákona o Národní komisi pro lidská práva.

([157]) Například pokud Národní komise pro lidská práva výjimečně nemůže prověřit určité materiály nebo zařízení, neboť se týkají státních tajemství, která by mohla mít podstatný vliv na bezpečnost státu nebo diplomatické vztahy, nebo pokud by inspekce představovala závažnou překážku pro vyšetřování trestné činnosti nebo probíhající soudní řízení (viz poznámka pod čarou č. 166), a pokud by to Národní komisi pro lidská práva bránilo provést šetření nezbytné k posouzení podstaty obdržené stížnosti, sdělí fyzické osobě důvody, proč byla stížnost zamítnuta, v souladu s článkem 39 zákona o Národní komisi pro lidská práva. V tomto případě by jednotlivec mohl rozhodnutí Národní komise pro lidská práva napadnout podle zákona o správním soudním řízení.

([158]) Viz např. rozhodnutí Vrchního soudu v Soulu 2007Nu27259, 18. dubna 2008, které potvrdilo rozhodnutí Nejvyššího soudu 2008Du7854, 9. října 2008; rozhodnutí Vrchního soudu v Soulu 2017Nu69382, 2. února 2018.

([159]) Články 121 a 219 zákona o trestním řízení.

([160]) Článek 417 zákona o trestním řízení ve spojení s čl. 414 odst. 2 zákona o trestním řízení. Viz rozhodnutí Nejvyššího soudu 97Mo66, 29. září 1997.

Kromě toho mohou fyzické osoby získat náhradu škody u korejského soudu. Podle zákona o náhradě škody státem mohou fyzické osoby žádat o náhradu škody způsobené státními úředníky při výkonu jejich služebních povinností v rozporu se zákonem ([161]). Žalobu podle zákona o náhradě škody státem lze podat u specializované „rady pro náhradu škody" nebo přímo u korejských soudů ([162]). Pokud je obětí cizí státní příslušník, zákon o náhradě škody státem se použije, jestliže země původu tohoto cizího státního příslušníka stejnou měrou zajišťuje náhradu škody státem pro korejské státní příslušníky ([163]). Podle judikatury je tato podmínka splněna, pokud požadavky na žádost o náhradu škody v druhé zemi *„nejsou mezi Koreou a druhou zemí výrazně nevyvážené"* a *„nejsou obecně přísnější než požadavky, které stanovila Korea, a nevykazují žádný podstatný a obsahový rozdíl"* ([164]). Občanský zákoník upravuje odpovědnost státu za náhradu škody a v důsledku toho se odpovědnost státu vztahuje také na nemajetkovou újmu (např. duševní utrpení) ([165]).

V případě porušení pravidel ochrany údajů je v zákoně o ochraně osobních údajů stanoven další opravný prostředek. Podle článku 39 zákona o ochraně osobních údajů může každá fyzická osoba, která utrpí újmu v důsledku porušení zákona o ochraně osobních údajů nebo ztráty, krádeže, prozrazení, padělání, pozměnění nebo poškození jejích osobních údajů, získat náhradu škody u soudu. Neexistuje obdobný požadavek reciprocity jako podle zákona o náhradě škody státem.

Kromě náhrady škody lze získat správní opravný prostředek týkající se jednání nebo nečinnosti správních orgánů podle zákona o správním soudním řízení. Každá fyzická osoba může napadnout opatření (tj. výkon nebo odmítnutí provést výkon veřejné moci v konkrétním případě) nebo nečinnost (pokud správní orgán dlouhodobě nejedná, ačkoli je ze zákona povinen tak učinit) a toto napadení může vést ke zrušení/změně protiprávního opatření, k prohlášení neplatnosti (tj. konstatování, že opatření nemá právní účinek nebo neexistuje v právním řádu) nebo ke zjištění protiprávnosti nečinnosti ([166]). Aby bylo možné napadnout správní opatření, musí mít přímý dopad na občanská práva a povinnosti ([167]). To zahrnuje opatření ke shromažďování osobních údajů, ať už přímo (např. odposlech komunikace), nebo prostřednictvím žádosti o zpřístupnění (např. poskytovateli služeb).

Výše uvedené nároky lze uplatnit nejprve u správních odvolacích komisí zřízených při některých orgánech veřejné správy (např. Národní zpravodajské služby, Národní komise pro lidská práva) nebo u Ústřední správní odvolací komise zřízené v rámci Komise pro boj proti korupci a občanská práva ([168]). Takovýto správní opravný prostředek nabízí alternativní, neformálnější způsob, jak napadnout opatření nebo nečinnost orgánu veřejné správy. Podle zákona o správním soudním řízení však lze také podat žalobu přímo u korejských soudů.

Žádost o zrušení/změnu opatření podle zákona o správním soudním řízení může podat každá osoba, která má právní zájem domáhat se zrušení/změny nebo navrácení svých práv zrušením/změnou, pokud již opatření není účinné ([169]). Obdobně může žalobu na prohlášení neplatnosti podat osoba, která má na takovém prohlášení právní zájem, přičemž k zahájení soudního řízení o potvrzení nezákonnosti může dát podnět každá osoba, která podala žádost o opatření a má právní zájem na potvrzení protiprávnosti nečinnosti ([170]). Podle judikatury Nejvyššího soudu je „právní zájem" vykládán jako „právem chráněný zájem", tj. přímý a konkrétní zájem chráněný právními a správními předpisy, na nichž jsou založena správní opatření (tj. nikoli obecné, nepřímé a abstraktní veřejné zájmy) ([171]). Fyzické osoby proto mají právní zájem v případě jakéhokoli porušení omezení a záruk týkajících se shromažďování jejich osobních údajů pro účely vymáhání trestního práva (podle zvláštních zákonů nebo zákona o ochraně osobních údajů). Pravomocný rozsudek podle zákona o správním soudním řízení je pro účastníky řízení závazný ([172]).

Návrh na zrušení/změnu opatření a návrh na potvrzení protiprávnosti nečinnosti musí být podán do 90 dnů ode dne, kdy se fyzická osoba o opatření/nečinnosti dozví, a to zpravidla nejpozději do jednoho roku ode dne vydání

([161]) Ustanovení čl. 2 odst. 1 zákona o náhradě škody státem.

([162]) Články 9 a 12 zákona o náhradě škody státem. Zákon zřizuje okresní rady (kterým předsedá náměstek státního zástupce příslušného státního zastupitelství), ústřední radu (které předsedá náměstek ministra spravedlnosti) a zvláštní radu (které předsedá náměstek ministra národní obrany a která vyřizuje nároky na náhradu škody způsobené vojenským personálem nebo civilními zaměstnanci armády). Žádosti o náhradu škody zpravidla vyřizují okresní rady, které musí za určitých okolností postoupit věc ústřední/zvláštní radě, např. pokud náhrada škody přesáhne určitou částku nebo pokud jednotlivec požádá o opětovné projednání. Všechny rady se skládají z členů jmenovaných ministrem spravedlnosti (např. z řad úředníků Ministerstva spravedlnosti, soudních znalců, advokátů a osob se zkušenostmi v oblasti náhrad škody státem) a podléhají zvláštním pravidlům pro střet zájmů (viz článek 7 prováděcí vyhlášky k zákonu o náhradě škody státem).

([163]) Článek 7 zákona o náhradě škody státem.

([164]) Rozhodnutí Nejvyššího soudu 2013Da208388, 11. června 2015.

([165]) Viz článek 8 zákona o náhradě škody státem a rovněž článek 751 občanského zákoníku.

([166]) Články 2 a 4 zákona o správním soudním řízení.

([167]) Rozhodnutí Nejvyššího soudu 98Du18435, 22. října 1999, rozhodnutí Nejvyššího soudu 99Du1113, 8. září 2000, a rozhodnutí Nejvyššího soudu 2010Du3541, 27. září 2012.

([168]) Článek 6 zákona o správních opravných prostředcích a čl. 18 odst. 1 zákona o správním soudním řízení.

([169]) Článek 12 zákona o správním soudním řízení.

([170]) Články 35 a 36 zákona o správním soudním řízení.

([171]) Rozhodnutí Nejvyššího soudu 2006Du330, 26. března 2006.

([172]) Ustanovení čl. 30 odst. 1 zákona o správním soudním řízení.

opatření / nečinnosti, neexistují-li důvody, které by to mohly ospravedlňovat ([173]). Podle judikatury Nejvyššího soudu je třeba výraz „přiměřené důvody“ vykládat široce a je zapotřebí posoudit, zda je společensky přijatelné připustit opožděnou stížnost s ohledem na všechny okolnosti dané věci ([174]). To například zahrnuje (mimo jiné) důvody prodlení, za které dotčená strana nemůže nést odpovědnost (tj. situace, které jsou mimo kontrolu stěžovatele, například pokud nebyl informován o shromažďování jeho osobních údajů), nebo vyšší moc (např. přírodní katastrofa, válka).

V neposlední řadě mohou ústavní stížnost Ústavnímu soudu podat i fyzické osoby ([175]). Na základě zákona o Ústavním soudu může kterákoli osoba, jejíž základní práva zaručená ústavou jsou porušena výkonem nebo nečinností vládní moci (vyjma soudních rozsudků), požádat o soudní rozhodnutí o ústavní stížnosti. Jsou-li k dispozici jiné opravné prostředky, musí být nejprve vyčerpány. Podle judikatury Ústavního soudu mohou cizí státní příslušníci podat ústavní stížnost v rozsahu, v jakém korejská ústava uznává jejich základní práva (viz vysvětlení v oddíle 1.1) ([176]). Ústavní stížnosti musí být podány do 90 dnů poté, co se fyzická osoba dozví o porušení práva, a do jednoho roku poté, co k tomuto porušení práva došlo. Vzhledem k tomu, že na řízení podle zákona o Ústavním soudu se použije postup podle zákona o správním soudním řízení ([177]), bude stížnost přípustná i v případě, že existují „přiměřené důvody“ ve smyslu výkladu v souladu s výše popsanou judikaturou Nejvyššího soudu.

Je-li nejprve nutné vyčerpat jiné opravné prostředky, musí být ústavní stížnost podána do 30 dnů po konečném rozhodnutí o takovém opravném prostředku ([178]). Ústavní soud může zneplatnit výkon vládní moci, který porušení práva způsobil, nebo potvrdit, že určitá nečinnost je protiústavní ([179]). V takovém případě je příslušný orgán povinen přijmout opatření, aby vyhověl rozhodnutí soudu.

3. PŘÍSTUP VLÁDY PRO ÚČELY NÁRODNÍ BEZPEČNOSTI

3.1. Příslušné orgány veřejné správy v oblasti národní bezpečnosti

Korejská republika má dvě specializované zpravodajské služby: Národní zpravodajskou službu a Velitelství podpory zabezpečení obrany. Kromě toho mohou osobní údaje pro účely národní bezpečnosti shromažďovat i policie a státní zástupci.

Národní zpravodajská služba je zřízena zákonem o Národní zpravodajské službě a podléhá přímo jurisdikci a dohledu prezidenta ([180]). Národní zpravodajská služba zejména shromažďuje, kompiluje a distribuuje informace o cizích zemích (a Severní Koreji) ([181]), zpravodajské informace související s bojem proti špionážní činnosti (včetně vojenské a průmyslové špionáže), terorismu a činnosti mezinárodních syndikátů páchajících trestnou činnost, zpravodajské informace o určitých druzích trestné činnosti namířené proti veřejné a národní bezpečnosti (např. vnitrostátní nepokoje, zahraniční agrese) a zpravodajské informace související se zajišťováním kybernetické bezpečnosti a s předcházením kybernetickým útokům a hrozbám či bojem proti nim ([182]). Zákon o Národní zpravodajské službě, kterým se zřizuje Národní zpravodajská služba a vymezují její úkoly, rovněž stanoví obecné zásady, které tvoří rámec všech činností služby. Obecně platí, že Národní zpravodajská služba musí zachovávat politickou neutralitu a chránit svobodu a práva jednotlivců ([183]). Předseda Národní zpravodajské služby je pověřen vypracováním obecných pokynů, které stanoví zásady, rozsah a postupy pro plnění povinností Národní zpravodajské služby, pokud jde o shromažďování a využívání informací, a musí tyto pokyny sdělit Národnímu shromáždění ([184]). Národní shromáždění (prostřednictvím svého zpravodajského výboru) může požadovat opravu nebo doplnění pokynů, pokud je považuje za nezákonné nebo nespravedlivé. Obecněji řečeno, ředitel a pracovníci Národní zpravodajské služby nesmí při plnění svých povinností zneužíváním své úřední pravomoci nutit žádnou instituci, organizaci nebo fyzickou osobu k ničemu, co není její povinností, ani bránit žádné osobě ve výkonu práv ([185]). Kromě toho jakákoli cenzura pošty, odposlech telekomunikačního provozu, shromažďování informací o poloze, shromažďování údajů potvrzujících komunikaci nebo nahrávání či odposlouchávání soukromé komunikace ze

([173]) Článek 20 zákona o správním soudním řízení. Tato lhůta platí i pro tvrzení protiprávnosti nečinnosti, viz čl. 38 odst. 2 zákona o správním soudním řízení.
([174]) Rozhodnutí Nejvyššího soudu 90Nu6521, 28. června 1991.
([175]) Ustanovení čl. 68 odst. 1 zákona o Ústavním soudu.
([176]) Rozhodnutí Ústavního soudu 99HeonMa194, 29. listopadu 2001.
([177]) Článek 40 zákona o Ústavním soudu.
([178]) Článek 69 zákona o Ústavním soudu.
([179]) Ustanovení čl. 75 odst. 3 zákona o Ústavním soudu.
([180]) Článek 2 a čl. 4 odst. 2 zákona o Národní zpravodajské službě.
([181]) Tento pojem nezahrnuje údaje o jednotlivcích, ale informace o obecných údajích týkajících se jiných zemí (trendy, vývoj) a o činnosti státních subjektů třetích zemí.
([182]) Ustanovení čl. 3 odst. 1 zákona o Národní zpravodajské službě.
([183]) Ustanovení čl. 3 odst. 1, čl. 6 odst. 2, článků 11 a 21. Viz také pravidla týkající se střetu zájmů, zejména články 10 a 12.
([184]) Ustanovení čl. 4 odst. 2 zákona o Národní zpravodajské službě.
([185]) Článek 13 zákona o Národní zpravodajské službě.

strany Národní zpravodajské služby musí být v souladu se zákonem o ochraně důvěrnosti komunikací, zákonem o údajích o poloze nebo zákonem o trestním řízení ([186]). Jakékoli zneužití pravomoci nebo shromažďování údajů v rozporu s těmito právními předpisy podléhá trestním sankcím ([187]).

Velitelství podpory zabezpečení obrany je vojenská zpravodajská služba zřízená Ministerstvem obrany. Nese odpovědnost za bezpečnostní záležitosti v rámci armády, vyšetřování trestných činů v armádě (na základě zákona o vojenském soudu) a vojenské zpravodajství. Velitelství podpory zabezpečení obrany obecně neprovádí sledování civilistů, není-li nezbytné pro výkon jeho vojenských funkcí. Vyšetřovanými osobami mohou být vojenský personál, civilní zaměstnanci armády, osoby ve vojenském výcviku, osoby v armádní záloze nebo náborové službě a váleční zajatci ([188]). Při shromažďování údajů o komunikaci pro účely národní bezpečnosti podléhá Velitelství podpory zabezpečení obrany omezením a zárukám plynoucím ze zákona o ochraně důvěrnosti komunikací a z prováděcí vyhlášky k tomuto zákonu.

3.2. **Právní základy a omezení**

Zákon o ochraně důvěrnosti komunikací, zákon o boji proti terorismu na ochranu občanů a veřejné bezpečnosti (dále jen „zákon o boji proti terorismu“) a zákon o telekomunikačních službách představují právní základy pro shromažďování osobních údajů pro účely národní bezpečnosti a stanoví příslušná omezení a záruky ([189]). Tato omezení a záruky, jak jsou popsány v dalších oddílech, zajišťují, aby bylo shromažďování a zpracování údajů omezeno na to, co je nezbytně nutné k dosažení legitimního cíle. Je tak vyloučeno jakékoli masové a neselektivní shromažďování osobních údajů nebo přístup k těmto osobním údajům z důvodu národní bezpečnosti.

3.2.1. *Shromažďování údajů o komunikaci*

3.2.1.1. Shromažďování údajů o komunikaci zpravodajskými službami

3.2.1.1.1. Právní základ

Zákon o ochraně důvěrnosti komunikací opravňuje zpravodajské služby ke shromažďování údajů o komunikaci a vyžaduje, aby poskytovatelé komunikačních služeb spolupracovali podle požadavků těchto služeb ([190]). Jak je popsáno v oddíle 2.2.2.1, zákon o ochraně důvěrnosti komunikací rozlišuje mezi shromažďováním obsahu komunikace (tj. „*opatřeními omezujícími komunikaci*“, jako jsou opatření typu „*odposlech*“ nebo „*cenzura*“ ([191])), a shromažďováním „*údajů potvrzujících komunikaci*“ ([192]).

Prahová hodnota pro shromažďování těchto dvou druhů údajů se liší, použitelné postupy a záruky jsou však do značné míry totožné ([193]). Shromažďování údajů potvrzujících komunikaci (nebo příslušných metadat) může probíhat za účelem předcházení hrozbám pro národní bezpečnost ([194]). Vyšší prahová hodnota platí pro provádění opatření omezujících komunikaci (tj. shromažďování obsahu komunikace), která lze přijmout pouze v případě, že se očekává závažné ohrožení národní bezpečnosti a shromažďování zpravodajských informací je nezbytné k tomu, aby se takovému nebezpečí zabránilo (tj. pokud existuje závažné riziko pro národní bezpečnost a shromažďování údajů je nezbytné k předcházení tomuto riziku) ([195]). Kromě toho lze přístup k obsahu komunikace provádět pouze jako opatření poslední instance k zajištění národní bezpečnosti a je třeba usilovat o minimalizaci narušení soukromí komunikace ([196]). I pokud je získáno příslušné schválení/povolení, musí být taková opatření okamžitě ukončena, jakmile již nejsou nezbytná, aby se tak zajistilo, že jakékoli porušení komunikačních tajemství jednotlivce bude omezeno na minimum ([197]).

3.2.1.1.2. Omezení a záruky vztahující se na shromažďování údajů o komunikaci, které zahrnuje alespoň jednoho korejského státního příslušníka

Shromažďování údajů o komunikaci (obsahu i metadat), kdy jedna nebo obě fyzické osoby zapojené do komunikace jsou korejskými státními příslušníky, může probíhat pouze se svolením předsedy vrchního

([186]) Článek 14 zákona o Národní zpravodajské službě.
([187]) Články 22 a 23 zákona o Národní zpravodajské službě.
([188]) Článek 1 zákona o vojenském soudu.
([189]) Při vyšetřování trestných činů týkajících se národní bezpečnosti budou policie a Národní zpravodajská služba jednat na základě zákona o trestním řízení, zatímco Velitelství podpory zabezpečení obrany podléhá zákonu o vojenském soudu.
([190]) Článek 15-2 zákona o ochraně důvěrnosti komunikací.
([191]) Ustanovení čl. 2 odst. 6 a 7 zákona o ochraně důvěrnosti komunikací.
([192]) Ustanovení čl. 2 odst. 11 zákona o ochraně důvěrnosti komunikací.
([193]) Viz také čl. 13-4 odst. 2 zákona o ochraně důvěrnosti komunikací a čl. 37 odst. 4 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací, které stanoví, že postupy platné pro shromažďování obsahu komunikace se obdobně použijí na shromažďování údajů potvrzujících komunikaci.
([194]) Článek 13-4 zákona o ochraně důvěrnosti komunikací.
([195]) Ustanovení čl. 7 odst. 1 zákona o ochraně důvěrnosti komunikací.
([196]) Ustanovení čl. 3 odst. 2 zákona o ochraně důvěrnosti komunikací.
([197]) Článek 2 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.

soudu ([198]). Žádost zpravodajské služby musí být podána písemně státnímu zástupci nebo vrchnímu státnímu zastupitelství ([199]). Musí uvádět důvody pro shromažďování údajů (tj. že se očekává závažné ohrožení národní bezpečnosti nebo že je shromažďování údajů nezbytné, aby se předešlo ohrožení národní bezpečnosti), spolu s materiály podporujícími tyto důvody a nasvědčujícími důvodům prima facie, jakož i podrobnosti žádosti (tj. cíle, cílovou/é osobu/y, rozsah, dobu shromažďování údajů a také způsob a místo shromažďování údajů) ([200]). Státní zástupce / státní zastupitelství si pak vyžádá povolení předsedy vrchního soudu ([201]). Předseda vrchního soudu může udělit písemný souhlas pouze tehdy, pokud považuje žádost za odůvodněnou, a žádost zamítne, pokud ji považuje za bezdůvodnou ([202]). Soudní příkaz upřesňuje druh, cíl, účel, rozsah a dobu vlastního shromažďování údajů, stejně jako povolené místo a způsob shromažďování údajů ([203]).

Zvláštní pravidla platí v případě, že se opatření zaměřuje na vyšetřování zločinného spolčení, které ohrožuje národní bezpečnost, a nastane mimořádná událost, kvůli které nelze uskutečnit všechny výše uvedené postupy ([204]). Jsou-li tyto podmínky splněny, mohou zpravodajské služby provádět sledování bez předchozího souhlasu soudu ([205]). Ihned po provedení mimořádných opatření si však zpravodajská služba musí vyžádat souhlas soudu. Není-li souhlas získán do 36 hodin od přijetí opatření, musí být opatření okamžitě ukončena ([206]). Shromažďování údajů v mimořádných situacích musí vždy probíhat v souladu s „prohlášením o mimořádné cenzuře/odposlechu“ a zpravodajská služba, která provádí shromažďování údajů, musí vést registr všech mimořádných opatření ([207]).

V případech, kdy je sledování dokončeno v krátké době, a není proto možné získat souhlas soudu, musí vedoucí představitel příslušného vrchního státního zastupitelství zaslat oznámení o mimořádném opatření vypracované zpravodajskou službou předsedovi příslušného soudu, který vede registr mimořádných opatření ([208]). To soudu umožní prověřit zákonnost shromažďování údajů.

3.2.1.1.3. Omezení a záruky vztahující se na shromažďování údajů o komunikaci, které zahrnuje pouze cizí státní příslušníky

Ke shromažďování údajů o komunikaci výhradně mezi cizími státními příslušníky musí zpravodajské služby získat předchozí písemný souhlas prezidenta ([209]). Takové komunikační údaje budou pro účely národní bezpečnosti shromažďovány pouze tehdy, pokud spadají do jedné z několika vyjmenovaných kategorií, tj. komunikace mezi vládními úředníky nebo jinými osobami ze zemí nepřátelských vůči Korejské republice, zahraničními agenturami, skupinami nebo státními příslušníky podezřelými z účasti na činnostech zaměřených proti Koreji ([210]) nebo příslušníky skupin na Korejském poloostrově mimo oblast svrchovanosti Korejské republiky a jejich zastřešujícími skupinami se sídlem v zahraničí ([211]). Naopak, pokud je jedna strana komunikace korejským státním příslušníkem a druhá nekorejským státním příslušníkem, bude vyžadován souhlas soudu v souladu s postupem popsaným v oddíle 3.2.1.1.2.

Vedoucí představitel zpravodajské služby musí řediteli Národní zpravodajské služby předložit plán opatření, která mají být přijata ([212]). Ředitel Národní zpravodajské služby přezkoumá, zda je plán vhodný, a pokud tomu tak je, předloží jej ke schválení prezidentovi ([213]). Údaje, které musí být zahrnuty v plánu, jsou totožné s údaji požadovanými pro žádost o souhlas soudu se shromažďováním informací o korejských státních příslušnících (popsanými výše) ([214]). Zejména musí plán uvádět důvody pro shromažďování údajů (tj. že se očekává závažné ohrožení národní bezpečnosti nebo že je shromažďování údajů nezbytné, aby se předešlo ohrožení národní bezpečnosti), hlavní důvody podezření spolu

([198]) Ustanovení čl. 7 odst. 1 bodu 1 zákona o ochraně důvěrnosti komunikací. Příslušným soudem je vrchní soud s jurisdikcí podle místa bydliště nebo sídla jedné nebo obou stran, které jsou předmětem sledování.
([199]) Ustanovení čl. 7 odst. 3 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([200]) Ustanovení čl. 7 odst. 3 a čl. 6 odst. 4 zákona o ochraně důvěrnosti komunikací.
([201]) Ustanovení čl. 7 odst. 4 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací. Žádost státního zástupce podaná soudu musí obsahovat hlavní důvody podezření, a pokud je požadováno několik povolení současně, jejich odůvodnění (viz článek 4 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací).
([202]) Ustanovení čl. 7 odst. 3, čl. 6 odst. 5 a 9 zákona o ochraně důvěrnosti komunikací.
([203]) Ustanovení čl. 7 odst. 3 a čl. 6 odst. 6 zákona o ochraně důvěrnosti komunikací.
([204]) Článek 8 zákon o ochraně důvěrnosti komunikací.
([205]) Ustanovení čl. 8 odst. 1 zákona o ochraně důvěrnosti komunikací.
([206]) Ustanovení čl. 8 odst. 2 zákona o ochraně důvěrnosti komunikací.
([207]) Ustanovení čl. 8 odst. 4 zákona o ochraně důvěrnosti komunikací. Mimořádná opatření v kontextu vymáhání práva viz oddíl 2.2.2.2 výše.
([208]) Ustanovení čl. 8 odst. 5 a 7 zákona o ochraně důvěrnosti komunikací. V oznámení musí být uveden cíl, účel, rozsah, doba, místo a způsob shromažďování údajů, jakož i důvody pro nepodání žádosti před přijetím opatření (čl. 8 odst. 6 zákona o ochraně důvěrnosti komunikací).
([209]) Ustanovení čl. 7 odst. 1 bodu 2 zákona o ochraně důvěrnosti komunikací.
([210]) Jedná se o činnosti, které ohrožují existenci a bezpečnost národa, demokratický řád nebo přežití a svobodu lidí.
([211]) Pokud je navíc jedna strana osobou popsanou v čl. 7 odst. 1 bodě 2 zákona o ochraně důvěrnosti komunikací a druhá je neznámá nebo ji nelze specifikovat, použije se postup stanovený v čl. 7 odst. 1 bodě 2.
([212]) Ustanovení čl. 8 odst. 1 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací. Ředitele Národní zpravodajské služby jmenuje prezident po potvrzení parlamentem (článek 7 zákona o Národní zpravodajské službě).
([213]) Ustanovení čl. 8 odst. 2 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([214]) Ustanovení čl. 8 odst. 3 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací ve spojení s čl. 6 odst. 4 zákona o ochraně důvěrnosti komunikací.

s materiály podporujícími tyto důvody a nasvědčujícími důvodům *prima facie*, jakož i podrobnosti žádosti (tj. cíle, cílovou/é osobu/y, rozsah, dobu shromažďování údajů a také způsob a místo shromažďování údajů). Je-li požadováno několik souhlasů současně, jejich význam a důvody ([215]).

V mimořádných situacích ([216]) je třeba získat předchozí souhlas ministra, do jehož gesce náleží příslušná zpravodajská služba. V tomto případě si však zpravodajská služba musí vyžádat souhlas prezidenta ihned po přijetí mimořádných opatření. Pokud zpravodajská služba nezíská souhlas do 36 hodin od podání žádosti, musí být shromažďování údajů okamžitě ukončeno ([217]). V takových případech budou shromážděné údaje vždy zničeny.

3.2.1.1.4. Obecné zásady a záruky

Při žádosti o součinnost soukromých subjektů jim zpravodajské služby musí předložit soudní příkaz / souhlas prezidenta nebo kopii průvodního dopisu k prohlášení o mimořádné cenzuře, které musí dožádaný subjekt uchovat ve své evidenci ([218]). Subjekty, které jsou na základě zákona o ochraně důvěrnosti komunikací požádány o zpřístupnění informací zpravodajským službám, mohou zpřístupnění odmítnout, pokud povolení nebo prohlášení o mimořádné cenzuře odkazuje na nesprávný identifikátor (např. telefonní číslo patřící jiné než identifikované osobě). Kromě toho nesmí být nikdy zpřístupněna hesla používaná pro komunikaci ([219]).

Zpravodajské služby mohou prováděním opatření omezujících komunikaci nebo shromažďováním údajů potvrzujících komunikaci pověřit poštu nebo poskytovatele telekomunikačních služeb (ve smyslu zákona o telekomunikacích) ([220]). Příslušná zpravodajská služba i poskytovatel, který obdrží žádost o spolupráci, musí vést registry s uvedením účelu žádosti o opatření, data provedení nebo spolupráce a předmětu opatření (např. pošta, telefon, e-mail) po dobu tří let ([221]). Poskytovatelé telekomunikačních služeb, kteří poskytují údaje potvrzující komunikaci, musí ve své evidenci uchovávat informace o četnosti shromažďování údajů po dobu sedmi let a dvakrát ročně podávat zprávy ministrovi pro vědu a IKT ([222]).

Zpravodajské služby musí řediteli Národní zpravodajské služby oznamovat, jaké údaje shromáždily a jaký je výstup sledování ([223]). Pokud jde o shromažďování údajů potvrzujících komunikaci, musí být evidovány záznamy o podání žádosti o taková data, jakož i písemná žádost sama a instituce, která ji využila ([224]).

Shromažďování obsahu komunikace i údajů potvrzujících komunikaci může trvat po dobu nejvýše čtyř měsíců, a je-li mezitím dosaženo sledovaného cíle, musí být okamžitě ukončeno ([225]). Pokud podmínky pro povolení trvají, může být tato lhůta prodloužena až o čtyři měsíce, a to se souhlasem soudu nebo prezidenta. Žádost o souhlas s prodloužením opatření týkajících se sledování musí být podána písemně s uvedením důvodů, proč se o prodloužení žádá, a s poskytnutím podpůrných materiálů ([226]).

Podle právního základu shromažďování jsou fyzické osoby obecně vyrozuměny, jsou-li shromažďovány údaje o jejich komunikaci. Vedoucí představitel zpravodajské služby musí dotčenou osobu o sledování písemně informovat do 30 dnů ode dne, kdy sledování skončilo, zejména bez ohledu na to, zda se shromážděné informace týkají obsahu komunikace nebo údajů potvrzujících komunikaci, a bez ohledu na to, zda byly informace získány běžným postupem, nebo v mimořádné situaci ([227]). Oznámení musí obsahovat 1) skutečnost, že byly shromážděny údaje; 2) výkonnou agenturu

([215]) Ustanovení čl. 8 odst. 3 a 4 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([216]) Tj. v případech, kdy je cílem opatření akt spolčení ohrožující národní bezpečnost, není dostatek času na získání souhlasu prezidenta a nepřijetí mimořádných opatření může poškodit národní bezpečnost (čl. 8 odst. 8 zákona o ochraně důvěrnosti komunikací).
([217]) Ustanovení čl. 8 odst. 9 zákona o ochraně důvěrnosti komunikací.
([218]) Ustanovení čl. 9 odst. 2 zákona o ochraně důvěrnosti komunikací a článku 12 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([219]) Ustanovení čl. 9 odst. 4 zákona o ochraně důvěrnosti komunikací.
([220]) Článek 13 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([221]) Ustanovení čl. 9 odst. 3 zákona o ochraně důvěrnosti komunikací a čl. 17 odst. 2 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací. Tato lhůta se nepoužije na údaje potvrzující komunikaci (viz článek 39 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací).
([222]) Ustanovení čl. 13 odst. 7 zákona o ochraně důvěrnosti komunikací a článku 39 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([223]) Ustanovení čl. 18 odst. 3 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([224]) Ustanovení čl. 13 odst. 5 a čl. 13-4 odst. 3 zákona o ochraně důvěrnosti komunikací.
([225]) Ustanovení čl. 7 odst. 2 zákona o ochraně důvěrnosti komunikací.
([226]) Ustanovení čl. 7 odst. 2 zákona o ochraně důvěrnosti komunikací a článku 5 prováděcí vyhlášky k zákonu o ochraně důvěrnosti komunikací.
([227]) Ustanovení čl. 9-2 odst. 3 zákona o ochraně důvěrnosti komunikací. V souladu s článkem 13-4 zákona o ochraně důvěrnosti komunikací to platí jak pro shromažďování obsahu komunikace, tak pro údaje potvrzující komunikaci.

a 3) dobu výkonu opatření. Pokud je však pravděpodobné, že by oznámení ohrozilo národní bezpečnost nebo by znamenalo újmu na životě a fyzické bezpečnosti osob, lze oznámení odložit ([228]). Oznámení musí být podáno do 30 dnů, jakmile pominou důvody odkladu ([229]).

Tato oznamovací povinnost se však vztahuje pouze na shromažďování údajů, kdy je alespoň jedna ze stran korejským státním příslušníkem. V důsledku toho budou jiní než korejští státní příslušníci uvědoměni pouze v případě, že budou shromážděny údaje o jejich komunikaci s korejskými státními příslušníky. Neexistuje tedy žádná oznamovací povinnost, pokud se shromažďují údaje o komunikaci výhradně mezi jinými než korejskými státními příslušníky.

Obsah jakékoli komunikace, jakož i údaje potvrzující komunikaci získané sledováním na základě zákona o ochraně důvěrnosti komunikací lze použít pouze 1) pro vyšetřování, trestní stíhání nebo prevenci určitých trestných činů; 2) pro disciplinární řízení; 3) pro soudní řízení, v němž se na tyto údaje strana související s komunikací odvolává v rámci nároku na náhradu škody, nebo 4) na základě jiných právních předpisů ([230]).

3.2.1.2. Shromažďování údajů o komunikaci policií / státními zástupci pro účely národní bezpečnosti

Policie/státní zástupce může shromažďovat údaje o komunikaci (obsah komunikace i údaje potvrzující komunikaci) pro účely národní bezpečnosti za stejných podmínek, jaké jsou popsány v oddíle 3.2.1.1. Při jednání v mimořádných situacích ([231]) se použije postup, který byl popsán výše, pokud jde o shromažďování obsahu komunikace pro účely vymáhání práva v mimořádných situacích (tj. článek 8 zákona o ochraně důvěrnosti komunikací).

3.2.2. *Shromažďování údajů o osobách podezřelých z terorismu*

3.2.2.1. Právní základ

Zákon o boji proti terorismu dává řediteli Národní zpravodajské služby pravomoc shromažďovat informace o osobách podezřelých z terorismu ([232]). „*Osoba podezřelá z terorismu*“ je definována jako člen teroristické skupiny ([233]), osoba, která podporuje teroristickou skupinu (propagací a šířením myšlenek nebo taktiky teroristické skupiny), získává nebo vynakládá finanční prostředky na terorismus ([234]) nebo se zapojila do jiných činností v rámci přípravy, konspirace, propagace nebo podněcování terorismu, nebo osoba, u které existují oprávněné důvody pro podezření, že takovou činnost prováděla ([235]). Obecně platí, že každý veřejný činitel prosazující zákon proti terorismu musí respektovat základní práva zakotvená v korejské ústavě ([236]).

Zákon o boji proti terorismu sám o sobě nestanoví konkrétní pravomoci, omezení a záruky v oblasti shromažďování informací o osobách podezřelých z terorismu, odkazuje spíše na postupy stanovené v jiných právních předpisech. Zaprvé může na základě zákona o boji proti terorismu ředitel Národní zpravodajské služby shromažďovat 1) údaje o vstupu do Korejské republiky a opuštění Korejské republiky; 2) údaje o finančních transakcích a 3) údaje o komunikaci. V závislosti na druhu požadovaných informací jsou příslušné procesní požadavky stanoveny v imigračním zákoně a celním zákoně, v zákoně o oznamování a používání určitých informací o finančních transakcích, resp. v zákoně o ochraně důvěrnosti komunikací ([237]). Pro shromažďování údajů o vstupu do Koreje a opuštění Koreje odkazuje zákon o boji proti terorismu na postupy stanovené v imigračním a celním zákoně. Uvedené akty však v současnosti

([228]) Ustanovení čl. 9-2 odst. 4 zákona o ochraně důvěrnosti komunikací.
([229]) Ustanovení čl. 13-4 odst. 2 a čl. 9-2 odst. 6 zákona o ochraně důvěrnosti komunikací.
([230]) Ustanovení čl. 5 odst. 1 a 2 a článků 12 a 13-5 zákona o ochraně důvěrnosti komunikací.
([231]) To znamená, že cílem opatření je akt spolčení, který ohrožuje národní bezpečnost, a existuje mimořádná situace, kvůli které nelze uskutečnit běžný schvalovací postup (čl. 8 odst. 1 zákona o ochraně důvěrnosti komunikací).
([232]) Článek 9 zákona o boji proti terorismu.
([233]) „*Teroristická skupina*“ je definována jako skupina teroristů označená Organizací spojených národů (čl. 2 odst. 2 zákona o boji proti terorismu).
([234]) „*Terorismus*“ je v čl. 2 odst. 1 zákona o boji proti terorismu definován jako jednání prováděné za účelem bránění výkonu pravomoci státu, místní správy nebo zahraniční vlády (včetně místních správ a mezinárodních organizací) nebo s cílem přimět tyto subjekty k jednání, které není jejich povinností, nebo zastrašit veřejnost. To zahrnuje a) usmrcení osoby nebo ohrožení života osoby způsobením tělesné újmy nebo zatčením, zadržením, únosem nebo vzetím osoby jako rukojmí; b) určité druhy jednání cílené na letadlo (např. havárie, únos nebo poškození letadla za letu); c) určité druhy jednání související s plavidlem (např. obsazení lodi nebo provozního námořního zařízení, zničení lodi nebo provozního námořního zařízení nebo jejich poškození takového stupně, že je ohrožena jejich bezpečnost, včetně poškození nákladu plavidla nebo provozního námořního zařízení); d) umístění, odpálení nebo jiné použití biochemické, výbušné nebo zápalné zbraně nebo zařízení s úmyslem způsobit smrt, závažné zranění nebo závažné materiální škody nebo takto zasáhnout určité druhy vozidel nebo zařízení (např. vlaky, tramvaje, motorová vozidla, veřejné parky a nádraží, zařízení pro dodávku elektřiny, plynu a telekomunikační zařízení atd.); e) určité druhy jednání týkající se jaderných materiálů, radioaktivních materiálů nebo jaderných zařízení (např. způsobení újmy na životech či zdraví lidí nebo majetku nebo jiné narušení veřejné bezpečnosti zničením jaderného reaktoru nebo neoprávněnou manipulací s radioaktivními materiály atd.).
([235]) Ustanovení čl. 2 odst. 3 zákona o boji proti terorismu.
([236]) Ustanovení čl. 3 odst. 3 zákona o boji proti terorismu.
([237]) Ustanovení čl. 9 odst. 1 zákona o boji proti terorismu.

takové pravomoci nestanoví. Pro shromažďování údajů o komunikaci a údajů o finančních transakcích odkazuje zákon o boji proti terorismu na omezení a záruky uvedené v zákoně o ochraně důvěrnosti komunikací (které jsou podrobněji popsány níže) a zákoně o oznamování a používání určitých informací o finančních transakcích (který, jak je vysvětleno v oddíle 2.1, není pro posouzení pro účely rozhodnutí o odpovídající ochraně relevantní).

Kromě toho čl. 9 odst. 3 protiteroristického zákona stanoví, že ředitel Národní zpravodajské služby může od správce osobních údajů ([238]) nebo poskytovatele údajů o poloze ([239]) požadovat osobní údaje nebo údaje o poloze osoby podezřelé z terorismu. Tato možnost je omezena na žádosti o dobrovolné zpřístupnění údajů, na které nejsou správci osobních údajů a poskytovatelé údajů o poloze povinni reagovat, přičemž v každém případě tak mohou učinit pouze v souladu se zákonem o ochraně osobních údajů a zákonem o údajích o poloze (viz oddíl 3.2.2.2 níže).

3.2.2.2. Omezení a záruky vztahující se na dobrovolné zpřístupnění podle zákona o ochraně osobních údajů a zákona o údajích o poloze

Žádosti o dobrovolnou spolupráci podle zákona o boji proti terorismu musí být omezeny na informace o osobách podezřelých z terorismu (viz bod 3.2.2.1 výše). Jakákoli taková žádost Národní zpravodajské služby musí být v souladu se zásadami zákonnosti, nezbytnosti a proporcionality vyplývajícími z korejské ústavy (čl. 12 odst. 1 a čl. 37 odst. 2) ([240]) a rovněž s požadavky zákona o ochraně osobních údajů týkajícími se shromažďování osobních údajů (čl. 3 odst. 1 zákona o ochraně osobních údajů, viz oddíl 1.2 výše). Zákon o Národní zpravodajské službě dále upřesňuje, že Národní zpravodajská služba nesmí zneužíváním své úřední pravomoci nutit žádnou instituci, organizaci nebo fyzickou osobu k ničemu, co není její povinností, ani bránit žádné osobě ve výkonu práv ([241]). Porušení tohoto zákazu může podléhat trestním sankcím ([242]).

Správci osobních údajů a poskytovatelé údajů o poloze, kteří obdrží žádosti Národní zpravodajské služby na základě zákona o boji proti terorismu, nejsou povinni žádostem vyhovět. Mohou vyhovět dobrovolně, ale smí tak činit pouze v souladu se zákonem o ochraně osobních údajů a zákonem o údajích o poloze. Pokud jde o soulad se zákonem o ochraně osobních údajů, správce musí zejména vzít v úvahu zájmy subjektu údajů a nesmí tyto informace zpřístupnit, pokud by to mohlo nekorektním způsobem narušit zájem jednotlivce nebo třetí strany ([243]). Kromě toho musí být v souladu s oznámením č. 2021-1 o doplňkových pravidlech pro výklad a použití zákona o ochraně osobních údajů o zpřístupnění údajů informována dotčená osoba. Ve výjimečných situacích může být takové oznámení odloženo, zejména pokud a dokud by ohrozilo probíhající vyšetřování trestného činu nebo by pravděpodobně způsobilo újmu na životě či zdraví jiné osoby, přičemž tato práva nebo tyto zájmy jsou zjevně nadřazeny právům subjektu údajů ([244]).

3.2.2.3. Omezení a záruky podle zákona o ochraně důvěrnosti komunikací

Na základě zákona o boji proti terorismu mohou zpravodajské služby shromažďovat údaje o komunikaci (obsah komunikace i údaje potvrzující komunikaci), pouze pokud je to nezbytné pro protiteroristické činnosti, tedy činnosti související s předcházením terorismu a opatřeními v rámci boje proti terorismu. Postupy zákona o ochraně důvěrnosti komunikací popsané v oddíle 3.2.1 se vztahují na shromažďování údajů o komunikaci pro účely boje proti terorismu.

3.2.3. *Dobrovolné zpřístupnění ze strany poskytovatelů telekomunikačních služeb*

Na základě zákona o telekomunikačních službách mohou poskytovatelé telekomunikačních služeb vyhovět žádosti o zpřístupnění „komunikačních údajů“ ze strany zpravodajské služby, která hodlá shromáždit informace, aby zabránila ohrožení národní bezpečnosti ([245]). Každá taková žádost musí být v souladu se zásadami zákonnosti, nezbytnosti a proporcionality vyplývajícími z korejské ústavy (čl. 12 odst. 1 a čl. 37 odst. 2) ([246]) a rovněž s požadavky zákona o ochraně osobních údajů týkajícími se shromažďování osobních údajů (čl. 3 odst. 1 zákona o ochraně osobních údajů, viz oddíl 1.2 výše). Kromě toho platí stejná omezení a záruky jako pro dobrovolné zpřístupnění pro účely vymáhání práva (viz oddíl 2.2.3) ([247]).

([238]) Jak je definován v článku 2 zákona o ochraně osobních údajů, tj. veřejná instituce, právnická osoba, organizace, fyzická osoba atd., která přímo nebo nepřímo zpracovává osobní údaje za účelem používání souborů osobních údajů pro úřední nebo obchodní účely.

([239]) Jak je definován v článku 5 zákona o ochraně, používání a jiném nakládání s údaji o poloze (dále jen „zákon o údajích o poloze“), tj. kdokoli, kdo získal povolení od Korejské komise pro komunikace k podnikání v oblasti informací o poloze.

([240]) Viz rovněž čl. 3 odst. 2 a 3 zákona o boji proti terorismu.

([241]) Ustanovení čl. 11 odst. 1 zákona o Národní zpravodajské službě.

([242]) Článek 19 zákona o Národní zpravodajské službě.

([243]) Ustanovení čl. 18 odst. 2 zákona o ochraně osobních údajů.

([244]) Oznámení Komise pro ochranu osobních údajů č. 2021-1 o doplňkových pravidlech pro výklad a použití zákona o ochraně osobních údajů, oddíl III bod 2 podbod iii).

([245]) Ustanovení čl. 83 odst. 3 zákona o telekomunikačních službách.

([246]) Viz rovněž čl. 3 odst. 2 a 3 zákona o boji proti terorismu.

([247]) Žádost musí být zejména písemná a musí v ní být uvedeny důvody žádosti, dále odkaz na příslušného uživatele a rozsah požadovaných údajů, přičemž poskytovatel telekomunikačních služeb musí vést záznamy a dvakrát za rok podávat zprávy ministrovi pro vědu a IKT.

Poskytovatelé telekomunikačních služeb nejsou povinni žádosti vyhovět, mohou tak ale učinit dobrovolně a pouze v souladu se zákonem o ochraně osobních údajů. V tomto ohledu se na poskytovatele telekomunikačních služeb, kteří obdrželi žádosti donucovacích orgánů, vztahují stejné povinnosti, a to i pokud jde o oznámení fyzické osobě, jak je podrobněji vysvětleno v oddíle 2.2.3.

3.3. **Dozor**

Dohled nad činností korejských zpravodajských služeb vykonávají různé subjekty. Dohled nad Velitelstvím podpory zabezpečení obrany zajišťuje Ministerstvo národní obrany v souladu se směrnicí ministerstva o provádění vnitřního auditu. Národní zpravodajská služba podléhá dohledu ze strany výkonné moci, Národního shromáždění a dalších nezávislých subjektů, jak je podrobněji vysvětleno níže.

3.3.1. *Pověřenec pro ochranu lidských práv*

Pokud zpravodajské služby shromažďují informace o osobách podezřelých z terorismu, zákon o boji proti terorismu stanoví dohled ze strany Komise pro boj proti terorismu a pověřence pro ochranu lidských práv ([248]).

Komise pro boj proti terorismu mimo jiné vypracovává politiky týkající se protiteroristických aktivit a dohlíží na provádění protiteroristických opatření i na činnost různých příslušných orgánů v oblasti boje proti terorismu ([249]). Komisi předsedá předseda vlády a tvoří ji několik ministrů a vedoucích představitelů vládních agentur, včetně ministra zahraničních věcí, ministra spravedlnosti, ministra národní obrany, ministra vnitra a bezpečnosti, ředitele Národní zpravodajské služby, generálního komisaře Národní policejní agentury a předsedy Komise pro finanční služby ([250]). Při provádění vyšetřování v rámci boje proti terorismu a pátrání po osobách podezřelých z terorismu za účelem shromažďování údajů nebo materiálů nezbytných pro protiteroristické činnosti musí ředitel Národní zpravodajské služby podat zprávu předsedovi Komise pro boj proti terorismu (tj. předsedovi vlády) ([251]).

Zákon o boji proti terorismu dále zřizuje funkci pověřence pro ochranu lidských práv, který má chránit základní práva fyzických osob před porušováním způsobeným protiteroristickými činnostmi ([252]). Pověřence pro ochranu lidských práv jmenuje předseda Komise pro boj proti terorismu z řad fyzických osob, které splňují požadavky na způsobilost uvedené v prováděcí vyhlášce k zákonu o boji proti terorismu (tj. kdokoli s kvalifikací advokáta a nejméně desetiletou praxí nebo osoba s odbornou znalostí v oblasti lidských práv, která nejméně deset let pracuje nebo pracovala (alespoň) jako vysokoškolský docent nebo jako vyšší státní úředník ve státních agenturách nebo orgánech místní správy, nebo osoba s nejméně desetiletou pracovní praxí v oblasti lidských práv, např. v nevládní organizaci) ([253]). Pověřenec pro ochranu lidských práv je jmenován na dva roky (s možností prodloužení funkčního období) a může být z funkce odvolán pouze ze specifických, omezených a oprávněných důvodů, např. je-li obžalován v trestní věci související s jeho povinnostmi, při vyzrazení důvěrných informací nebo z důvodu dlouhodobé duševní či fyzické nezpůsobilosti ([254]).

Z hlediska pravomocí může pověřenec pro ochranu lidských práv vydávat doporučení ke zlepšení ochrany lidských práv ze strany agentur zapojených do protiteroristických činností a vyřizovat stížnosti občanů (viz oddíl 3.4.3) ([255]). Pokud lze důvodně prokázat porušení lidských práv při plnění úředních povinností, může pověřenec pro ochranu lidských práv doporučit vedoucímu představiteli odpovědné agentury, aby toto porušení napravil ([256]). Odpovědná agentura je pak povinna informovat pověřence pro ochranu lidských práv o opatřeních přijatých k realizaci takového doporučení ([257]). Pokud by agentura nerealizovala doporučení pověřence pro ochranu lidských práv, byla by záležitost postoupena komisi, včetně jejího předsedy, tedy předsedy vlády. Dosud se nevyskytly případy, kdy by doporučení pověřence pro ochranu lidských práv nebyla provedena.

3.3.2. *Národní shromáždění*

Jak je popsáno v oddíle 2.3.2, Národní shromáždění může vyšetřovat orgány veřejné správy a provádět jejich inspekce a v této souvislosti požadovat zpřístupnění dokumentů a vynutit si účast svědků. Pokud jde o záležitosti spadající do jurisdikce Národní zpravodajské služby, tento parlamentní dohled provádí zpravodajský výbor Národního shromáždění ([258]). Ředitel Národní zpravodajské služby, který dohlíží na plnění povinností služby, podává zprávy

([248]) Článek 7 zákona o boji proti terorismu.
([249]) Ustanovení čl. 5 odst. 3 zákona o boji proti terorismu.
([250]) Ustanovení čl. 3 odst. 1 prováděcí vyhlášky k zákonu o boji proti terorismu.
([251]) Ustanovení čl. 9 odst. 4 zákona o boji proti terorismu.
([252]) Článek 7 zákona o boji proti terorismu.
([253]) Ustanovení čl. 7 odst. 1 prováděcí vyhlášky k zákonu o boji proti terorismu.
([254]) Ustanovení čl. 7 odst. 3 prováděcí vyhlášky k zákonu o boji proti terorismu.
([255]) Ustanovení čl. 8 odst. 1 prováděcí vyhlášky k zákonu o boji proti terorismu.
([256]) Ustanovení čl. 9 odst. 1 prováděcí vyhlášky k zákonu o boji proti terorismu. Pověřenec pro ochranu lidských práv rozhoduje o přijetí doporučení autonomně, je však povinen oznámit tato doporučení předsedovi Komise pro boj proti terorismu.
([257]) Ustanovení čl. 9 odst. 2 prováděcí vyhlášky k zákonu o boji proti terorismu.
([258]) Článek 36 a čl. 37 odst. 1 bod 16 zákona o Národním shromáždění.

zpravodajskému výboru (a rovněž prezidentovi) ([259]). Zpravodajský výbor si také může vyžádat zprávu o konkrétní záležitosti, na kterou je ředitel Národní zpravodajské služby povinen neprodleně odpovědět ([260]). Odmítnout odpověď nebo odmítnout vypovídat před zpravodajským výborem pro zpravodajství může pouze v případě, že jde o státní tajemství týkající se vojenských a diplomatických záležitostí nebo záležitostí souvisejících se Severní Koreou, pokud by zveřejnění mohlo mít vážný dopad na osud země ([261]). V tomto případě může zpravodajský výbor požádat o vysvětlení předsedu vlády. Není-li takové vysvětlení předloženo do sedmi dnů od podání žádosti, odpověď nebo výpověď již nelze odmítnout.

Pokud Národní shromáždění zjistí, že došlo k nezákonné nebo nevhodné činnosti, může požádat, aby příslušný orgán veřejné správy přijal nápravná opatření, včetně přiznání odškodného, přijetí disciplinárních opatření a zlepšení vnitřních postupů ([262]). Na základě takové žádosti musí orgán neprodleně jednat a oznámit výsledek Národnímu shromáždění. Existují zvláštní pravidla týkající se parlamentního dohledu, pokud jde o používání opatření omezujících komunikaci (tj. shromažďování obsahu komunikace) podle zákona o ochraně důvěrnosti komunikací ([263]). Pokud jde o posledně jmenované záležitosti, může Národní shromáždění požádat vedoucí představitele zpravodajských služeb o zprávu o jakémkoli konkrétním opatření omezujícím komunikaci. Kromě toho může provádět kontroly odposlouchávacích zařízení na místě. A v neposlední řadě musí zpravodajské služby, které shromáždily údaje o obsahu, a provozovatelé, kteří zpřístupnili údaje o obsahu pro účely národní bezpečnosti, na žádost Národního shromáždění podat o takovém zpřístupnění zprávu.

3.3.3. *Rada pro audit a inspekce*

Rada pro audit a inspekce vykonává ve vztahu ke zpravodajským službám stejné funkce dohledu jako v oblasti prosazování trestního práva (viz oddíl 2.3.2) ([264]).

3.3.4. *Komise pro ochranu osobních údajů*

Pokud jde o zpracování údajů pro účely národní bezpečnosti, včetně fáze shromažďování, vykonává další dozor Komise pro ochranu osobních údajů. Jak je podrobněji vysvětleno v oddíle 1.2, tento dozor zahrnuje obecné zásady a povinnosti stanovené v článku 3 a čl. 58 odst. 4 zákona o ochraně osobních údajů, jakož i výkon individuálních práv zaručených článkem 4 zákona o ochraně osobních údajů. Kromě toho se podle čl. 7-8 odst. 3 a 4 a čl. 7-9 odst. 5 zákona o ochraně osobních údajů dozor Komise pro ochranu osobních údajů vztahuje rovněž na možná porušení pravidel stanovených ve zvláštních právních předpisech vymezujících omezení a záruky v oblasti shromažďování osobních údajů, jako je zákon o ochraně důvěrnosti komunikací, zákon o boji proti terorismu a zákon o telekomunikačních službách. Vzhledem k požadavkům uvedeným v čl. 3 odst. 1 zákona o ochraně osobních údajů, pokud jde o zákonné a korektní shromažďování osobních údajů, představuje jakékoli porušení uvedených zákonů porušení zákona o ochraně osobních údajů. Komise pro ochranu osobních údajů má tedy pravomoc vyšetřovat ([265]) porušení právních předpisů upravujících přístup k údajům pro účely národní bezpečnosti, jakož i pravidel zpracování podle zákona o ochraně osobních údajů, a vydávat doporučení ke zlepšení, ukládat nápravná opatření, doporučovat disciplinární opatření a předkládat případné přestupky příslušným vyšetřovacím orgánům ([266]).

3.3.5. *Národní komise pro lidská práva*

Dohled ze strany Národní komise pro lidská práva se vztahuje stejným způsobem na zpravodajské služby i na jiné vládní orgány (viz oddíl 2.3.2).

3.4. **Individuální ochrana**

3.4.1. *Opravné prostředky u pověřence pro ochranu lidských práv*

Pokud jde o shromažďování osobních údajů v souvislosti s protiteroristickými činnostmi, zajišťuje zvláštní možnost opravných prostředků pověřenec pro ochranu lidských práv, jehož funkce je zřízena v rámci Komise pro boj proti terorismu. Pověřenec pro ochranu lidských práv vyřizuje občanské stížnosti týkající se porušování lidských práv v důsledku protiteroristických činností ([267]). Může doporučit nápravné opatření a příslušná agentura musí pověřenci oznámit všechna opatření přijatá k provedení takového doporučení. Pro podání stížnosti pověřenci pro ochranu lidských práv není stanoven žádný vstupní požadavek. Pověřenec pro ochranu lidských práv se proto bude stížností zabývat, i pokud dotčená osoba nemůže ve fázi posouzení přípustnosti prokázat újmu.

([259]) Článek 18 zákona o Národní zpravodajské službě.
([260]) Ustanovení čl. 15 odst. 2 zákona o Národní zpravodajské službě.
([261]) Ustanovení čl. 17 odst. 2 zákona o Národní zpravodajské službě. „Státní tajemství" jsou definována jako „*skutečnosti, věci nebo znalosti klasifikované jako státní tajemství, k nimž je přístup povolen omezenému okruhu osob a které nesmějí být vyzrazeny žádné jiné zemi nebo organizaci, aby se předešlo závažnému narušení národní bezpečnosti*", viz čl. 13 odst. 4 zákona o Národní zpravodajské službě.
([262]) Ustanovení čl. 16 odst. 2 zákona o inspekci a vyšetřování ve státní správě.
([263]) Článek 15 zákon o ochraně důvěrnosti komunikací.
([264]) Stejně jako v případě zpravodajského výboru Národního shromáždění může ředitel Národní zpravodajské služby odmítnout odpovědět Radě pro audit a inspekce, pouze pokud jde o záležitosti, které představují státní tajemství, a v případě, že by zveřejnění mělo závažný dopad na národní bezpečnost (čl. 13 odst. 1 zákona o Národní zpravodajské službě).
([265]) Článek 63 zákona o ochraně osobních údajů.
([266]) Ustanovení čl. 61 odst. 2, čl. 65 odst. 1 a 2 a čl. 64 odst. 4 zákona o ochraně osobních údajů.
([267]) Ustanovení čl. 8 odst. 1 bodu 2 prováděcí vyhlášky k zákonu o boji proti terorismu.

3.4.2. *Ochranné mechanismy dostupné podle zákona o ochraně osobních údajů*

Pokud jde o osobní údaje zpracovávané pro účely národní bezpečnosti, mohou jednotlivci vykonávat svá práva na přístup, opravu, výmaz a pozastavení zpracování podle zákona o ochraně osobních údajů ([268]). Žádosti týkající se výkonu těchto práv lze podávat přímo zpravodajské službě, nebo nepřímo prostřednictvím Komise pro ochranu osobních údajů. Zpravodajská služba může toto právo pozdržet, omezit nebo odepřít, pokud je to nezbytné a přiměřené k ochraně důležitého cíle veřejného zájmu (například v takovém rozsahu a po takovou dobu, kdy by udělení práva ohrozilo probíhající vyšetřování nebo ohrozilo národní bezpečnost), nebo pokud udělení práva může způsobit újmu na životě nebo zdraví třetí strany. Pokud je žádost zamítnuta nebo omezena, musí být fyzické osobě neprodleně oznámeny příslušné důvody.

Kromě toho v souladu s čl. 58 odst. 4 zákona o ochraně osobních údajů (požadavek na zajištění náležitého vyřízení individuálních stížností) a čl. 4 odst. 5 zákona o ochraně osobních údajů (právo na přiměřenou náhradu jakékoli škody vzniklé v důsledku zpracování osobních údajů, a to prostřednictvím rychlého a spravedlivého řízení) mají fyzické osoby právo na nápravu. To zahrnuje právo oznámit údajné porušení kontaktnímu centru pro oznamování případů porušení ochrany osobních údajů a podat stížnost Komisi pro ochranu osobních údajů ([269]). Tyto opravné prostředky jsou k dispozici v případě možného porušení pravidel obsažených ve zvláštních právních předpisech, kterými se stanoví omezení a záruky týkající se shromažďování osobních údajů pro účely národní bezpečnosti, a porušení zákona o ochraně osobních údajů. Jak je vysvětleno v oznámení č. 2021-1, fyzická osoba z EU může podat stížnost Komisi pro ochranu osobních údajů prostřednictvím svého vnitrostátního orgánu pro ochranu údajů. V takovém případě Komise pro ochranu osobních údajů prostřednictvím vnitrostátního úřadu pro ochranu osobních údajů informuje dotčenou osobu, jakmile je vyšetřování ukončeno (případně včetně informací o uložených nápravných opatřeních). Proti rozhodnutím nebo nečinnosti Komise pro ochranu osobních údajů lze dále podat opravný prostředek u korejských soudů podle zákona o správním soudním řízení.

3.4.3. *Opravné prostředky u Národní komise pro lidská práva*

Možnost individuálního opravného prostředku u Národní komise pro lidská práva se vztahuje stejným způsobem na zpravodajské služby i na jiné vládní orgány (viz oddíl 2.4.2).

3.4.4. *Soudní ochrana*

Stejně jako v případě činností donucovacích orgánů mohou fyzické osoby získat soudní ochranu vůči zpravodajským službám ve věci porušení výše uvedených omezení a záruk různými způsoby.

Zaprvé mohou fyzické osoby získat náhradu škody podle zákona o náhradě škody státem. Například v jednom případě bylo poskytnuto odškodnění za nezákonné sledování ze strany Velitelství podpory obrany (předchůdce Velitelství podpory zabezpečení obrany) ([270]).

Zadruhé zákon o správním soudním řízení umožňuje fyzickým osobám napadnout opatření a nečinnost správních orgánů, včetně zpravodajských služeb ([271]).

A konečně mohou také fyzické osoby podat ústavní stížnost na opatření přijatá zpravodajskými službami k Ústavnímu soudu na základě zákona o Ústavním soudu.

([268]) Čl. 3 odst. 5 a čl. 4 odst. 1, 3 a 4 zákona o ochraně osobních údajů.
([269]) Článek 62 a čl. 63 odst. 2 zákona o ochraně osobních údajů.
([270]) Rozhodnutí Nejvyššího soudu 96Da42789, 24. července 1998.
([271]) Články 3 a 4 zákona o správním soudním řízení.