ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.cz, www.uoou.cz

Čj. UOOU-03305/20-5

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 64 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů, a podle čl. 58 odst. 2 písm. i) 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), vydává dne 3. září 2020 v souladu s § 150 odst. 1 zákona č. 500/2004 Sb., správní řád, a § 90 odst. 1 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, tento příkaz:

Univerzita [redacted], se sídlem nám. [redacted]

I. se uznává vinnou ze spáchání přestupku podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb., neboť porušila některou z povinností podle čl. 8, 11, 25 až 39, 42 až 49 nařízení (EU) 2016/679 nebo hlavy II, kterého se, jako správce osobních údajů podle čl. 4 bodu 7 nařízení (EU) 2016/679, v rámci přijímacího řízení uchazečů o studium, dopustila tím, že zpracovávala rodné číslo pro účel přihlášení uchazeče o studium do informačního systému studijní agendy pouze v kombinaci s iniciálami uchazeče o studium, a to minimálně v období ode dne podání stížnosti, tedy 14. června 2019, do vyhotovení protokolu o kontrole, tedy 13. března 2020,

   čímž porušila povinnost stanovenou v čl. 32 odst. 1 nařízení (EU) 2016/679, tedy povinnost správce s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob provést vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku,

II. se uznává vinnou ze spáchání přestupku podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb., neboť porušila některou ze základních zásad pro zpracování osobních údajů podle čl. 5 až 7 nebo 9 nařízení (EU) 2016/679, kterého se, jako správce osobních údajů podle čl. 4 bodu 7 nařízení (EU) 2016/679, dopustila v rámci přijímacího řízení uchazečů o studium využitím rodného čísla pro účel přihlášení uchazeče o studium do informačního systému studijní agendy, a to minimálně v období ode dne podání stížnosti, tedy 14. června 2019, do vyhotovení protokolu o kontrole, tedy 13. března 2020,

čímž porušila zásadu zpracování osobních údajů stanovenou v čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679, tedy zásadu, že osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný („účelové omezení“),

III. se uznává vinnou ze spáchání přestupku podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb., neboť porušila některou ze základních zásad pro zpracování osobních údajů podle čl. 5 až 7 nebo 9 nařízení (EU) 2016/679, kterého se, jako správce osobních údajů podle čl. 4 bodu 7 nařízení (EU) 2016/679, v rámci přijímacího řízení uchazečů o studium dopustila tím, že nestanovila jednoznačný účel a právní základ pro zpracování osobních údajů v rozsahu shromažďovaných údajů kvalifikátor občanství, místo narození, informace, odkud se uchazeč hlásí a soukromý e-mail, a přesto tyto osobní údaje zpracovávala, a to minimálně v období ode dne podání stížnosti, tedy 14. června 2019, do vyhotovení protokolu o kontrole, tedy 13. března 2020,

čímž porušila povinnost stanovenou v čl. 6 odst. 1 nařízení (EU) 2016/679, tedy povinnost zákonného zpracování osobních údajů,

IV. se uznává vinnou ze spáchání přestupku podle § 62 odst. 1 písm. c) zákona č. 110/2019 Sb., neboť porušila některé z práv subjektu údajů podle čl. 12 až 22 nařízení (EU) 2016/679 nebo hlavy II, kterého se, jako správce osobních údajů podle čl. 4 bodu 7 nařízení (EU) 2016/679, v rámci přijímacího řízení uchazečů o studium dopustila tím, že poskytla subjektu údajů informace nepřesné ve vztahu k účelu a právnímu titulu pro zpracování osobních údajů, a to minimálně v období ode dne podání stížnosti, tedy 14. června 2019, do vyhotovení protokolu o kontrole, tedy 13. března 2020,

čímž porušila povinnost stanovenou v čl. 13 odst. 1 písm. c) nařízení (EU) 2016/679, tedy povinnost správce poskytnout v okamžiku získání osobní údajů informace o účelech zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování,

V. přičemž se podle § 62 odst. 5 zákona č. 110/2019 Sb.

upouští od uložení správního trestu.

Odůvodnění

Podkladem pro vydání tohoto příkazu je protokol o kontrole, č. j. UOOU-02808/19-35, ze dne 13. března 2020, a spisový materiál shromážděný v průběhu kontroly provedené u účastníka řízení, jímž je Univerzita [redacted] (dále jen „obviněná“), kontrolní skupinou Úřadu pro ochranu osobních údajů (dále jen „Úřad“) ve dnech od 25. října 2019 do 15. června 2020, včetně vyřízení námitek předsedkyní Úřadu, č. j. UOOU-02808/19-38, ze dne 11. června 2020.

Kontrola byla zahájena na základě stížnosti, přičemž předmětem kontroly bylo dodržování povinností stanovených obviněné nařízením (EU) 2016/679 a zákonem č. 110/2019 Sb.,

v souvislosti se zpracováním osobních údajů v rámci přijímacího řízení uchazečů o studium, včetně využití studijního informačního systému a jeho dodavatelů.

Provedenou kontrolou bylo konstatováno, že obviněná je správcem osobních údajů ve smyslu čl. 4 bod 7 nařízení (EU) 2016/679. Osobní údaje ve smyslu čl. 4 bod 2 nařízení (EU) 2016/679, vč. zvláštních kategorií osobních údajů dle čl. 9 nařízení (EU) 2016/679, v rámci procesu přijímacího řízení zpracovává ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679 elektronickou formou, prostřednictvím webové adresy eprihlaska.utb.cz, resp. prostřednictvím informačního systému pro podávání elektronické přihlášky.

K výroku I. správní orgán uvádí, že tímto bylo konstatováno, že obviněná porušila povinnost vyplývající z ustanovení čl. 32 nařízení (EU) 2016/679, a to tím, že z hlediska ochrany osobních údajů je přihlášení do informačního systému obviněné pomocí zadání rodného čísla pouze v kombinaci s iniciálami uchazeče o studium možným rizikem pro zabezpečení zpracování. Ze zavedeného způsobu přihlašování do informačního systému studijní agendy je evidentní, že každý, kdo bude znát rodné číslo uchazeče o studium, může v kombinaci s iniciálami jeho jména do prostřední elektronické přihlášky vstupovat, a tím přistupovat k jeho osobním údajům zde vyplněným, resp. s nimi též dále nakládat. Přihlášení není doplněno žádným heslem (ať už vygenerovaným či vytvořeným uchazečem o studium), ani není doplněno o žádnou další autentizaci.

Dle čl. 32 odst. 1 nařízení (EU) 2016/679 správce musí s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob provést vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, případně včetně opatření uvedených pod písm. a) až d) citovaného článku. Musí být zohledněna rizika, která zpracování představuje, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Je tedy zřejmé, že správce musí nejprve posoudit pravděpodobnost a závažnost rizik, která při zpracování osobních údajů hrozí, a následně s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování vybrat a následně zavést vhodná technická a organizační bezpečnostní opatření ke zmírnění těchto rizik. Riziko pro práva a svobody fyzických osob přitom lze považovat za kritérium, na němž závisí uplatnění nebo míra uplatnění řady institutů upravených v nařízení (EU) 2016/679. Riziko pro práva a svobody fyzických osob musí být hodnoceno na základě objektivního posouzení, kdy východiskem pro jeho posouzení je hrozba narušení důvěrnosti a integrity zpracování. Pro posouzení bezpečnostních rizik a volbu vhodných opatření k jejich zmírnění platí stejné zásady jako pro posuzování obecného rizika zpracování. Posouzení by nemělo být jednorázovým procesem, nýbrž by se mělo jednat o pravidelný proces vyhodnocování vnitřních a vnějších okolností, které mohou mít na míru rizika vliv, a v případě změny rizika pak musí správce bezpečnostní opatření zrevidovat a případně přijmout vhodnější.

Lze tedy shrnout, že splnění této povinnosti, tj. povinnosti provést vhodná technická a organizační opatření, aby byla zajištěna úroveň zabezpečení odpovídající danému riziku, aby osobní údaje nebyly vystaveny riziku neoprávněného zpracování či využití, předpokládá,

že účastník řízení důsledně zváží veškerá rizika, která jsou s jím prováděným zpracováním osobních údajů spojená, a přijme odpovídající opatření k jejich maximálnímu vyloučení.

K výroku II. správní orgán uvádí, že tímto bylo konstatováno, že obviněná porušila požadavek legitimního účelu zpracování osobních údajů vyplývající z ustanovení čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679, a to využitím rodného čísla pro účel přihlášení uchazeče o studium do informačního sytému studijní agendy.

Dle ustanovení čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679 musí být osobní údaje shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.

Z hlediska využití rodného čísla pro účel přihlášení uchazeče o studium do informačního systému studijní agendy jsou rozhodná ustanovení zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), kdy tento v § 13 odst. 9 stanoví, že rodné číslo je oprávněna užívat nebo rozhodovat o jeho využívání v mezích stanovených zákonem výlučně fyzická osoba, které bylo rodné číslo přiděleno (tj. nositel rodného čísla), nebo její zákonný zástupce, jinak lze rodné číslo využívat jen v případech stanovených v § 13c zákona o evidenci obyvatel. Využívání rodného čísla jakožto přihlašovacího údaje nesplňuje podmínky stanovené zákonem o evidenci obyvatel, vyjma situace, kdy by rodné číslo bylo takto využíváno se souhlasem nositele rodného čísla nebo jeho zákonného zástupce. Obviněná však neprokázala, že by souhlas k tomuto byl získáván. Využití rodného čísla pro účel přihlášení uchazeče o studium do informačního systému studijní agendy je tak v rozporu s ustanovením § 13c odst. 1 zákona o evidenci obyvatel a účel takového zpracování není legitimní, čímž je porušena zásada účelového omezení, zakotvená v čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679.

K výroku III. správní orgán uvádí, že tímto bylo konstatováno, že obviněná porušila povinnost zákonného zpracování osobních údajů ve smyslu čl. 6 odst. 1 nařízení (EU) 2016/679, dle kterého je zpracování zákonné, pouze pokud je splněna nejméně jedna z podmínek stanovených v písm. a) až f) tohoto ustanovení a pouze v odpovídajícím rozsahu. Obviněná jako správce osobních údajů neurčila jednoznačně účel a právní základ pro zpracování osobních údajů dle uvedeného článku. Uvedené se týká zpracování údajů kvalifikátor občanství, místo narození a informace, odkud se uchazeč hlásí, a dále údaje o rodinném stavu a soukromého e-mailu.

Vyplnění údajů kvalifikátor občanství, místo narození a informace, odkud se uchazeč hlásí, je v rámci elektronické přihlášky vyplňováno povinně, avšak zpracování těchto údajů není nezbytné, a proto by mohlo být prováděno pouze na základě právního titulu souhlasu, uděleného subjektem údajů. Tím však obviněná nedisponuje. Vyplnění údaje rodinný stav je nepovinné (resp. je defaultně nastaven na hodnotu „nezjištěn“), avšak není zřejmé, za jakým účelem by měl být zpracováván, pokud jej uchazeč o studium vyplní. Soukromý e-mail je v rámci elektronické přihlášky povinnou položkou. V současné době již lze do určité míry e-mailovou adresu považovat za údaj přidružený k běžným korespondenčním údajům a za jasně stanovenými účely by v rámci procesu přijímacího řízení mohlo být zpracování tohoto údaje opodstatněné. Obviněná však neurčila jednoznačně právní základ pro zpracování dle čl. 6 odst. 1 nařízení (EU) 2016/679 a ani účely, ke kterým má být soukromý e-mail využíván, nejsou zřejmé. Lze konstatovat, že obviněná sama v rámci

námitek proti kontrolním zjištěním k údajům kvalifikátor občanství, místo narození, informace, odkud se uchazeč hlásí, a údaj o rodinném stavu uvedla, že se již snaží docílit odstranění těchto údajů z elektronické přihlášky.

Dle ustanovení čl. 6 odst. 1 nařízení (EU) 2016/679 správce může osobní údaje zpracovávat pouze v případě, že mu k tomu svědčí alespoň jeden z právních titulů, které jsou stanoveny ve výše uvedeném článku dle písmen a) až f). Právní titul je podmínka, bez které není zpracování v žádném případě možné, resp. je od počátku nelegální.

K výroku IV. správní orgán uvádí, že tímto bylo konstatováno, že obviněná nesplnila povinnost zajištění informování subjektu údajů v souladu s čl. 13 odst. 1 písm. c) nařízení (EU) 2016/679, neboť v části poskytnutí informace o právním základu pro zpracování osobních údajů obviněná poskytla subjektům údajů informace nepřesné. Uvedené porušení povinností navazuje na pochybení související s určením právního titulu pro zpracování osobních údajů.

Dle ustanovení čl. 13 odst. 1 písm. c) nařízení (EU) 2016/679 je správce povinen informovat subjekt údajů o zpracování osobních údajů, které se tohoto subjektu údajů týkají. Informační povinnost má správce dle tohoto článku v případě, že osobní údaje získal přímo od subjektu údajů, tedy subjekt údajů své osobní údaje tomuto správci přímo poskytl. Aby bylo zpracování osobních údajů ze strany účastníka řízení, jakožto správce osobních údajů, řádné a korektní, musí být informace subjektu údajů poskytnuty tak, aby byla naplněna zásada spravedlivého a transparentního zpracování. Subjekt musí být informován o právním základu pro zpracování, na němž je toto založeno, přičemž je nezbytné, aby účastník řízení poskytl subjektům údajů v rámci plnění své informační povinnosti přesné informace o právním základu pro zpracování osobních údajů, a taktéž informoval o účelech tohoto zpracování.

Podle § 5 zákona č. 250/2016 Sb. je přestupkem škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin.

Úřad považuje ve smyslu § 150 odst. 1 správního řádu skutkové zjištění za dostatečné a na základě výše uvedeného považuje za prokázané, že obviněná porušila svým jednáním zásadu stanovenou v čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679, tedy povinnost shromažďovat osobní údaje pro určité, výslovně vyjádřené a legitimní účely, přičemž tyto osobní údaje nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný („účelové omezení“); dále porušila povinnost stanovenou v čl. 6 odst. 1 nařízení (EU) 2016/679, tedy povinnost zákonnosti zpracování osobních údajů; dále porušila povinnost zakotvenou v čl. 13 odst. 1 písm. c), tedy povinnost poskytnout v okamžiku získání osobních údajů subjektu údajů informace o účelech zpracování, pro které jsou osobní údaje určeny, a o právním základu zpracování; a dále porušila povinnost stanovenou v čl. 32 nařízení (EU) 2016/679, tedy povinnost týkající se zabezpečení zpracování osobních údajů; a proto rozhodl podle § 150 odst. 1 správního řádu ve spojení s § 90 odst. 1 zákona č. 250/2016 Sb. ve věci příkazem.

Z čl. 83 odst. 7 nařízení (EU) 2016/679 vyplývá, že aniž jsou dotčeny nápravné pravomoci dozorových úřadů podle čl. 58 odst. 2 tohoto nařízení, může každý členský stát stanovit

pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě.

Podle § 62 odst. 5 zákona č. 110/2019 Sb. Úřad upustí od uložení správního trestu také tehdy, jde-li o správce a zpracovatele uvedené v čl. 83 odst. 7 nařízení (EU) 2016/679. S ohledem na skutečnost, že obviněná je veřejným subjektem, tedy správce uvedený v čl. 83 odst. 7 nařízení (EU) 2016/679, upustil Úřad od uložení správního trestu.

Poučení:

V souladu s § 150 odst. 3 správního řádu lze u Úřadu pro ochranu osobních údajů proti tomuto příkazu podat ve lhůtě 8 dnů ode dne jeho doručení odpor, kterým se příkaz ruší a řízení pokračuje.

Příkaz je doručen dnem převzetí stejnopisu, nejpozději ale desátým dnem od jeho uložení na poště. V případě doručování do datové schránky je dnem doručení okamžik přihlášení oprávněné osoby do datové schránky, nejpozději ale desátý den ode dne dodání příkazu do datové schránky.

Praha, 3. září 2020

otisk
úředního
razítka

Ing. Helena Žemličková
vedoucí oddělení kontroly veřejného sektoru
(podepsáno elektronicky)