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-09072/18-14
Praha 09. ledna 2019

Protokol o kontrole

Kontrolní orgán:

Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, 170 00 Praha 7 (dále jen „Úřad“).

Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z čl. 58 odst. 1 písm. b) 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), ve spojení s § 2 odst. 2 a 3 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Kontrolující:

Mgr. et Mgr. Božena Čajková – inspektorka Úřadu, průkaz inspektora č. [redacted],

Josef Polák – pověřený zaměstnanec Úřadu, průkaz pověřeného zaměstnance č. [redacted],

Mgr. Iva Tomášková – pověřená zaměstnankyně Úřadu, průkaz pověřené zaměstnankyně č. [redacted]

(dále jen „kontrolující“).

Kontrolovaná osoba:

[redacted]

(dále jen „kontrolovaný“).

Předmět kontroly:

Předmětem kontroly je dodržování povinností správce osobních údajů stanovených nařízením (EU) 2016/679, v souvislosti s používáním technologie Face ID, se zaměřením na zákonnost tohoto zpracování, poskytování informací o tomto zpracování a zabezpečení zpracovávaných osobních údajů.

První kontrolní úkon:

Oznámení o zahájení kontroly čj. UOOU-09072/18-2, doručené kontrolovanému dne 26. září 2018.

Poslední kontrolní úkon:

Úřední záznam o kontrolním úkonu ze dne 19. prosince 2018, čj. UOOU-09072/18-13 pořízení podkladů z webových stránek kontrolovaného.

I. Přehled podkladů:

Protokol o kontrole se opírá o následující podklady a dokumenty, které byly pořízeny před zahájením kontroly a v jejím průběhu, popř. o dokumenty a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti:

1. Kontrolní plán Úřadu pro rok 2018, čj. UOOU-09072/18-1, 5 listů;
2. Protokol z ústního jednání ze dne 10. října 2018, čj. UOOU-09072/18-4, 2 listy, s přílohami:
    a. Pověření k zastupování – [redacted], 1 list,
    b. Souhlas se zněním protokolu, 1 list;
3. Vyjádření kontrolovaného doručené Úřadu dne 1. listopadu 2018, čj. UOOU-09072/18-6, 4 listy, s přílohami:
    a. Závěrečná zpráva ze šetření mimořádné události, 2 listy,
    b. Rámcová smlouva o poskytování služeb – [redacted], 21 listů,
    c. Technicko-organizační opatření k zabezpečení osobních údajů zpracovávaných v systému [redacted], 7 listů,
    d. Seznam přístupových oprávnění do systému [redacted] v rámci stavby „Rekonstrukce hlavní (historické) budovy [redacted], 1 list,
    e. Seznam přístupových oprávnění do systému [redacted] v rámci stavby [redacted], 1 list,
    f. Pověření zaměstnanců – osoby určené pro styk s osobními údaji, 18 listů,
    g. Seznam pracovníků (operátorů) společnosti [redacted], s.r.o., 1 list,
    h. Objednávky – stavba „Rekonstrukce hlavní (historické) budovy [redacted], 17 listů,
    i. Objednávka – stavba [redacted], 2 listy,
    j. Smlouva o dílo – provedení prací na stavbě, [redacted], s.r.o., 43 listů,
    k. Smlouva o dílo – provedení prací na stavbě, [redacted], 37 listů,

l. Informace o zpracování osobních údajů I, 1 list,
m. Informace o zpracování osobních údajů II, 1 list;

4. Úřední záznam o kontrolním úkonu ze dne 13. listopadu 2018, čj. UOOU-09072/18-8 – místní šetření na stavbě (rekonstrukce hlavní, historické, budovy [redacted], 1 list, s přílohami:
   a. Fotodokumentace – umístění informační tabule, 1 list,
   b. Fotodokumentace – informační tabule, 1 list,
   c. Fotodokumentace – rozpoznání neznámé osoby, 1 list,
   d. Fotodokumentace – kniha návštěv, 1 list;
5. Protokol z ústního jednání a místního šetření ze dne 28. listopadu 2018, čj. UOOU-09072/18-10, včetně přílohy (souhlas se zněním protokolu), 4 listy;
6. Vyjádření kontrolovaného doručené Úřadu dne 11. prosince 2018, čj. UOOU-09072/18-11, 1 list, s přílohami:
   a. Přehled logů s přístupy uživatelů do aplikace v období září – říjen 2018, 8 listů,
   b. Přehled logů s přístupy operátorů do aplikace v období září – listopad 2018, 5 listů,
   c. Záznamy o činnostech zpracování – Face ID, 1 list,
   d. Organizačně řídící norma č. [redacted] Ochrana osobních údajů, 4 listy,
   e. Záznamy o činnostech zpracování – přehled účelů zpracování, 1 list,
   f. Ukázka automaticky generovaných informací „Souhrn první úrovně“, 1 list,
   g. Dodatek č. 1 k rámcové smlouvě o poskytování služeb na stavbách, 1 list;
7. Organizačně řídící norma č. [redacted] Ochrana osobních údajů – novelizace ke dni [redacted], 5 listů;
8. Úřední záznam o kontrolním úkonu ze dne 19. prosince 2018, čj. UOOU-09072/18-13 – pořízení podkladů z webových stránek kontrolovaného, včetně přílohy Zásady zpracování osobních údajů, 4 listy.

V rámci kontroly je posuzováno výhradně zpracování osobních údajů v čase provedení kontroly a v rozsahu stanoveném v předmětu kontroly. Z výše uvedených podkladů pak byly pro kontrolní zjištění vyhodnoceny pouze ty části, v nichž jsou uvedeny relevantní informace ve vztahu k předmětu této kontroly.

II. Kontrolní zjištění:

Kontrola byla zahájena na základě Kontrolního plánu Úřadu pro rok 2018, kam byla zařazena za účelem bližšího prověření plnění povinností při zpracování osobních údajů, včetně zvláštních kategorií, shromažďovaných pomocí technologie rozpoznávání obličeje.

Kontrolní zjištění č. 1.

Kontrolující předně posuzovali, zda informace, které kontrolovaný v souvislosti s používáním technologie umožňující rozpoznání obličeje zpracovává, jsou osobními údaji ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, podle kterého se osobním údajem rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje,

síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Současně kontrolující hodnotili, zda kontrolovaný zpracovává také zvláštní kategorie osobních údajů, kterými jsou dle čl. 9 bod 1 nařízení (EU) 2016/679 osobní údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

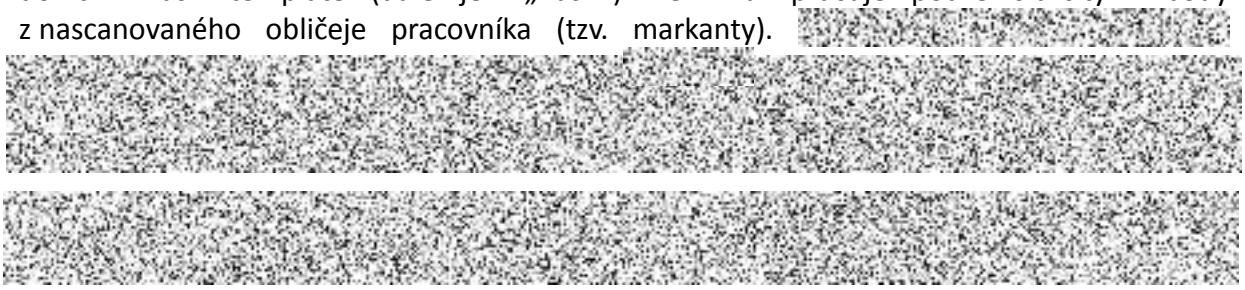
Kontrolou bylo zjištěno, že kontrolovaný používá na některých stavbách, které realizuje, zařízení určené k identifikaci pracovníků přítomných na stavbě pomocí technologie rozpoznání obličeje (dále jen „Face ID“). Pracovníci přítomní na stavbě jsou jak zaměstnanci kontrolovaného, tak zaměstnanci subdodavatelů, kteří se na stavbě podílejí na základě smlouvy o dílo (provedení prací na stavbě) uzavírané s kontrolovaným (podklady č. 3.j a 3.k).

Provoz Face ID zajišťuje pro kontrolovaného společnost [redacted], se sídlem [redacted] na základě Rámcové smlouvy ze [redacted] (dále jen „rámcová smlouva“) a na ní navazujících objednávek pro konkrétní stavbu. V době kontroly bylo Face ID používáno na dvou realizovaných stavbách, a to stavbě [redacted] a stavbě „Rekonstrukce hlavní (historické) budovy [redacted] (podklady č. 2, 3, 3.h a 3.i).

Face ID je docházkovým systémem umožňujícím zaznamenat čas příchodu a odchodu jednotlivých osob na stavbu pomocí rozpoznání obličeje. Jedná se o soubor turniketu, terminálu – čtecí (scanovací) jednotky a softwaru napojeného na server společnosti [redacted], k němuž se přistupuje prostřednictvím k tomu určené aplikace. Při instalaci Face ID na konkrétní stavbě určí kontrolovaný, konkrétně jeho zaměstnanec odpovědný za vedení stavby, osobu oprávněnou k přístupu do aplikace (dále jen „uživatel“). [redacted] (podklady č. 3.b, 3.c a 5).

Přístup jednotlivých pracovníků na stavbu pomocí Face ID zajišťuje uživatel tak, že se přihlásí do aplikace [redacted]. Operátor provede kontrolu údajů, potvrdí objednávku a vygeneruje ID pracovníka, které oznámí uživateli. Uživatel následně provede s daným pracovníkem, pod přiděleným ID, na terminálu umístěném na konkrétní stavbě prvotní scan obličeje. Tento scan je [redacted] převeden

do tzv. hash template (dále jen „hash“). Terminál pracuje pouze s určitými body z nascanovaného obličeje pracovníka (tzv. markanty).



V případě stavby „Rekonstrukce hlavní (historické) budovy je, na základě požadavku kontrolovaného, zaveden vyšší stupeň zabezpečení a

(podklady č. 4 a 5).

Seznam povolených pozic, tj. ID pracovníků oprávněných ke vstupu na stavbu, je z aplikace zasílán do terminálu. Údaje o docházce jsou naopak z terminálu v pravidelných intervalech zasílány do aplikace.

Kontrolovaný tedy prostřednictvím Face ID zpracovává jak identifikační údaje a profesní údaje zaměstnanců, tak i informace vypovídající o jejich pracovní docházce (blíže viz také kontrolní zjištění č. 6). Kontrolující proto konstatují, že kontrolovaný je pomocí Face ID schopen identifikovat pracovníky vstupující na stavbu. Identifikace jednotlivých osob vstupujících na stavbu je ostatně také účelem používání této technologie.

Zároveň je nutné konstatovat, že v souvislosti s účinností nařízení (EU) 2016/679, které mimo jiné zohledňuje vývoj technologií v oblasti zpracovávání osobních údajů, došlo ke změně v posuzování šablon biometrických údajů (hash), a jejich zpracování za účelem identifikace osob. Z pohledu nové právní regulace je nutno i využívání systémů pracujících s šablonami (tj. nikoli přímo s biometrickými údaji, ale jejich algoritmickým vyjádřením v podobě hash) považovat za zpracování zvláštních kategorií osobních údajů, které vyžadují zvláštní, resp. přísnější systém ochrany. Postup spočívající ve vytvoření a následném využívání hash biometrického údaje pak lze považovat za jeden z prvků zabezpečení, není však důvodem k vyjmutí ze zvláštních kategorií osobních údajů.

Kontrolující na základě výše uvedeného konstatují, že kontrolovaný zpracovává **osobní údaje** ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, a to včetně **zvláštních kategorií osobních údajů** ve smyslu čl. 9 bod 1 citovaného nařízení.

Kontrolní zjištění č. 2.

Kontrolující následně posoudili postavení kontrolovaného ve vztahu k čl. 4 bodu 7 nařízení (EU) 2016/679, dle kterého se správcem rozumí fyzická nebo právnická osoba, orgán veřejné moci,

agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.

Povinnost zpracovávat osobní údaje pracovníků, resp. osob přítomných na staveništi, vyplývá kontrolovanému ze zvláštních právních předpisů. Konkrétně se jedná o vedení evidence osob přítomných na staveništi dle zákona č. 309/2006 Sb., kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy (zákon o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci), a dále o evidenci osob pracujících na staveništi ve stavebním deníku dle vyhlášky Ministerstva pro místní rozvoj č. 499/2006 Sb., o dokumentaci staveb. Kontrolovanému dále vyplývají další povinnosti v oblasti zamezení nelegální práce dle zákona č. 435/2004 Sb., o zaměstnanosti. Dále je kontrolovaný povinen plnit povinnosti v oblasti evidence pracovní doby a zvyšování bezpečnosti práce a ochrany života a zdraví pracovníků dle zákona č. 262/2006 Sb., zákoník práce. Účel zpracování osobních údajů, který kontrolovaný sleduje prostřednictvím Face ID, je tak stanoven citovanými právními předpisy.

Prostředky zpracování – Face ID, resp. celý systém zahrnující jak zařízení umístěné na stavbě, tak aplikaci a server společnosti [redacted] – pak určil kontrolovaný v rámcové smlouvě (podklad č. 3.b), kde jako prostředek předmětného zpracování zvolil Face ID.

Na základě uvedených skutečností kontrolující konstatují, že kontrolovaný je v postavení **správce osobních údajů** dle čl. 4 bodu 7 nařízení (EU) 2016/679. Z tohoto titulu kontrolovaný primárně odpovídá za splnění všech požadavků vyplývajících z tohoto nařízení.

Kontrolní zjištění č. 3.

Kontrolující dále zjišťovali, zda se na předmětném zpracování podílí také zpracovatel osobních údajů, kterým je dle čl. 4 bod 8 nařízení (EU) fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

Jak již bylo uvedeno (viz kontrolní zjištění č. 1), poskytovatelem Face ID je společnost [redacted], se kterou za tímto účelem kontrolovaný uzavřel rámcovou smlouvu (podklad č. 3.b). Osobní údaje pracovníků jsou pak zpracovávány v aplikaci, resp. na serveru společnosti [redacted] jejími operátory, kteří zároveň nastavují přístupová práva do aplikace pro oprávněné pracovníky kontrolovaného (uživatele).

Z rozsahu a charakteru povinností, které společnosti [redacted] z rámcové smlouvy vyplývají, a z výše uvedeného popisu činnosti operátorů této společnosti je pak zřejmé, že společnost [redacted] poskytuje kontrolovanému služby spočívající ve shromažďování, uchovávání i dalším využívání osobních údajů prostřednictvím systému Face ID. Současně je zřejmé, že společnost [redacted] tuto činnost nerealizuje k dosažení vlastního cíle (účelu).

Kontrolující proto konstatují, že ve vztahu k předmětnému zpracování je společnost [redacted] v postavení **zpracovatele osobních údajů**, neboť zpracovává osobní údaje pro kontrolovaného.

Kontrolní zjištění č. 4.

V návaznosti na předchozí kontrolní zjištění kontrolující hodnotili, zda kontrolovaný uzavřel se společností [redacted] smlouvu o zpracování osobních údajů, jak je jeho povinností dle čl. 28 odst. 3 nařízení (EU) 2016/679, a zda tato smlouva splňuje požadované náležitosti.

Jak již bylo uvedeno, společnost [redacted] zajišťuje provoz Face ID pro kontrolovaného na základě rámcové smlouvy, v níž jsou popsány jednotlivé prvky Face ID, postupy pro zprovoznění terminálu a jeho demontáž, vkládání informací do aplikace, podmínky pro zpřístupnění aplikace, servisní zásahy, školení uživatelů aj.

Problematika zpracování osobních údajů je upravena v čl. [redacted] rámcové smlouvy. Dle tohoto ustanovení zpracovává společnost [redacted] pro kontrolovaného osobní údaje v rozsahu zde uvedeném (viz kontrolní zjištění č. 1.) za účelem plnění zákonných povinností kontrolovaného v oblasti bezpečnosti práce a zaměstnanosti dle zvláštních právních přepisů. Společnost [redacted] je povinna zpracovávat osobní údaje pouze na základě doložených pokynů kontrolovaného a není oprávněna zapojit ke zpracování dalšího zpracovatele. Společnost [redacted] se dále zavazuje:

- přijmout a zdokumentovat dostatečná technická a organizační opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení, ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování či zneužití,
- vydáním vlastních vnitřních předpisů, příp. prostřednictvím zvláštních smluvních ujednání, zajistit dodržování bezpečnostních opatření a mlčenlivosti ze strany osob, které u ní zpracovávají osobní údaje dle rámcové smlouvy,
- po skončení stavby a protokolárním odebrání terminálu osobní údaje získané na základě rámcové smlouvy zlikvidovat, vyjma údajů nutných pro prokázání povinnosti řádného vedení stavebního deníku dle zvláštních právních předpisů,
- umožnit kontrolovanému na jeho výzvu přístup k záznamům o činnostech zpracování osobních údajů a provést kontrolu technických a organizačních bezpečnostních opatření a jednotlivých operací zpracování osobních údajů v prostorách společnosti [redacted].

Smluvní strany se v rámcové smlouvě dále zavazují ke vzájemnému informování a potřebné součinnosti v případech neoprávněného či nezákonného zpracování osobních údajů, jejich poškození, ztráty, zničení, znehodnocení či jiného narušení zabezpečení.

Na základě uvedených skutečností kontrolující konstatují, že kontrolovaný uzavřel se společností [redacted] smlouvu o zpracování osobních údajů, resp. problematika zpracování osobních údajů je upravena v rámcové smlouvě, přičemž předmětná ujednání splňují náležitosti smlouvy o zpracování osobních údajů. Kontrolovaný tedy povinnost dle čl. 28 odst. 3 nařízení (EU) 2016/679 **neporušil**.

Kontrolní zjištění č. 5.

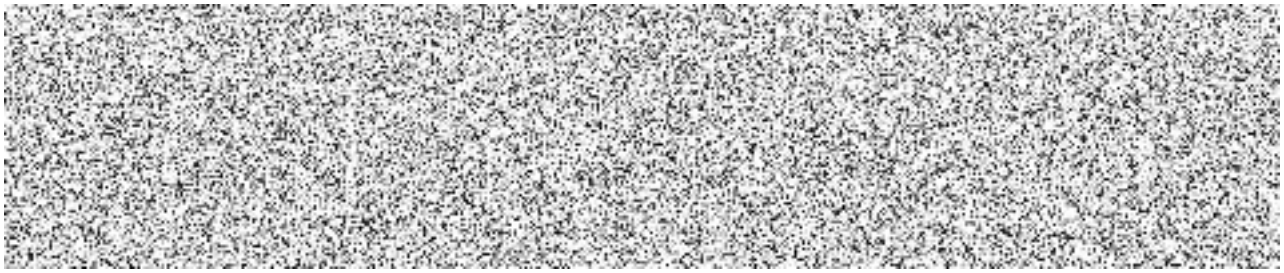
Kontrolující dále hodnotili, zda je pro zpracování osobních údajů, včetně zvláštních kategorií osobních údajů, v souvislosti s používáním Face ID dán právní titul, jak je požadován v čl. 6 a ve vztahu ke zvláštním kategoriím osobních údajů současně i v čl. 9 nařízení (EU) 2016/679 (při zpracování zvláštních kategorií osobních údajů je nutné, aby správce disponoval jak některým z obecných právních titulů, tak i právním titulem pro zpracování zvláštních kategorií údajů).

Jak již bylo uvedeno (viz kontrolní zjištění č. 2), kontrolovaný zpracovává předmětné osobní údaje za účelem plnění povinností stanovených zvláštními právními předpisy. Konkrétně se jedná o povinnost vést evidenci přítomnosti zaměstnanců a dalších fyzických osob na staveništi dle zákona č. 309/2006 Sb. a evidenci jmen a příjmení osob pracujících na staveništi ve stavebním deníku dle přílohy č. 16 vyhlášky č. 499/2006 Sb. Na kontrolovaného se dále vztahují povinnosti v oblasti zamezení nelegální práce dle zákona č. 435/2004 Sb. Dále je kontrolovaný povinen zajistit bezpečnost práce a ochranu života a zdraví pracovníků dle zákona č. 262/2006 Sb. Právním titulem pro zpracování osobních údajů pracovníků na stavbě je tedy zpracování nezbytné pro splnění právní povinnosti správce dle čl. 6 odst. 1 písm. c) nařízení (EU) 2016/679.

Ve vztahu ke zpracování biometrických údajů za účelem jednoznačné identifikace v rámci docházkových systémů je Úřad obecně toho názoru, že takové zpracování by mělo být využíváno pouze ve výjimečných situacích, kdy jiné řešení – spočívající v prosté evidenci osob – není s ohledem na specifické okolnosti dostačující. Tento požadavek – minimalizace rozsahu osobních údajů ve spojení s minimalizací zásahu do práv subjektů údajů – patří ostatně mezi základní zásady zpracování osobních údajů, které jsou v současné době vyjádřeny v čl. 5 odst. 1 nařízení (EU) 2016/679.

V tomto konkrétním případě lze dle kontrolujících zohlednit zejména specifický charakter pracoviště (staveniště) ve vztahu k povinnostem kontrolovaného souvisejícím se zajištěním bezpečnosti a ochrany života a zdraví při práci dle zákona č. 262/2006 Sb. Dle § 101 tohoto zákona je kontrolovaný jako zaměstnavatel povinen zajistit bezpečnost a ochranu zdraví zaměstnanců s ohledem na rizika možného ohrožení jejich života a zdraví při výkonu práce. Tuto povinnost je pak kontrolovaný povinen plnit ve vztahu ke všem zaměstnancům, kteří se s jeho vědomím na pracovišti zdržují. Dle § 3 odst. 2 písm. g) zákona č. 309/2006 Sb. kontrolovaný dále, jako zhotovitel stavby, odpovídá za splnění požadavků na způsobilost fyzických osob konajících práce na staveništi.

Vzhledem k tomu, že na staveniště vstupují nejen zaměstnanci kontrolovaného, ale také pověření zaměstnanci subdodavatelů (podklady č. 3, 3.j a 3.k), je dle § 101 odst. 4 zákona č. 262/2006 Sb. kontrolovaný povinen také zajistit, aby jeho činnosti a práce jeho zaměstnanců byly organizovány, koordinovány a prováděny tak, aby současně byli chráněni také zaměstnanci dalšího zaměstnavatele.



Dále je na místě zohlednit skutečnost, že na stavbách se podílejí také pracovníci – cizinci, přičemž z tohoto titulu vznikají kontrolovanému další povinnosti v oblasti zamezení nelegální práce. Dle § 141a zákona č. 435/2004 Sb. ručí právnická nebo fyzická osoba (příjemce plnění, tj. v tomto případě kontrolovaný) až do výše 10 000 000,- Kč za úhradu pokuty uložené právnické nebo fyzické osobě, která poskytla právnické nebo fyzické osobě v rámci obchodního vztahu plnění jako subdodavatel (přímo nebo prostřednictvím jiné osoby) a umožnila cizinci výkon nelegální práce dle § 5 písm. e) bodu 3 tohoto zákona. Toto ručení pak vzniká v případě, pokud příjemce plnění o nelegální práci věděl nebo při vynaložení náležité péče vědět měl a mohl. V případě zaměstnání cizince bez platného povolení k zaměstnání kontrolovanému dále hrozí riziko spočívající v úhradě nákladů spojených se správním vyhoštěním cizince (§ 123 zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů). V zájmu kontrolovaného tak je zajistit jednoznačnou identifikaci těchto osob, resp. vyloučit případnou záměnu.

Jak bylo popsáno výše, systém Face ID umožňuje vstup na pracoviště pouze osobám, které byly v systému zaevidovány jako oprávněné ke vstupu na dané staveniště, přičemž jejich identita je ověřována s využitím technologie rozpoznání obličeje umožňující jednoznačnou identifikaci osob a v zásadě vylučující záměnu.

S ohledem na výše uvedené kontrolující konstatují, že zpracování zvláštních kategorií osobních údajů (biometrických údajů ve formě hashe vytvořeného ze scanu obličeje) osob vstupujících na stavbu lze s ohledem na výše popsané okolnosti považovat za nezbytné za účelem plnění povinností kontrolovaného v oblasti pracovního práva, konkrétně zajištění bezpečnosti a ochrany života a zdraví osob na pracovišti. Zpracování je tak v tomto případě možné na základě čl. 9 odst. 2 písm. b) nařízení (EU) 206/679 ve spojení s čl. 6 odst. 1 písm. c) tohoto nařízení.

Na základě uvedených skutečností kontrolující konstatují, že kontrolovaný povinnosti stanovené v čl. 6 a 9 nařízení (EU) 2016/679 **neporušil**.

Kontrolní zjištění č. 6.

Kontrolující dále hodnotili, zda kontrolovaný zpracovává prostřednictvím Face ID osobní údaje pouze v rozsahu nezbytném ve vztahu k účelu tohoto zpracování, jak je jeho povinností dle čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679.

Jak je uvedeno v kontrolním zjištění č. 2, povinnost zpracovávat osobní údaje zaměstnanců, resp. osob přítomných na stavbě, vyplývá kontrolovanému ze zvláštních právních předpisů, tj. plnění povinností uložených kontrolovanému není bez zpracování popsaných osobních údajů možné či dostatečně účinné.

V situaci, kdy je zpracování osobních údajů založeno na právním titulu uvedeném v čl. 6 odst. 1 písm. c) tohoto nařízení a současně příslušné právní předpisy neupravují výslovný rozsah osobních údajů, jimiž je možno zákonnou povinnost naplnit, je povinností kontrolovaného – na základě 5 odst. 1 písm. c) nařízení (EU) 2016/679 – jakožto správce osobních údajů definovat takový okruh osobních údajů, jejichž zpracování bude k naplnění zákonných povinností dostačující.

Kontrolou bylo zjištěno (viz také kontrolní zjištění č. 1), že kontrolovaný v souvislosti s používáním technologie Face ID na stavbě zpracovává údaje o zaměstnancích v tomto rozsahu:

- identifikační údaje (titul, jméno, příjmení, vygenerované ID),
- profesní údaje (pracovní pozice, údaje o zaměstnavateli),
- v případě cizinců ze zemí mimo EU národnost a číslo a datum platnosti pracovního povolení a povolení k pobytu,
- informace o docházce na pracoviště (čas a směr průchodu přes turniket),
- hash vytvořený ze scanu obličeje (uchovávaný pouze v terminálu).

Po srovnání právních povinností kontrolovaného a uvedeného rozsahu osobních údajů a s odkazem na závěry popsané výše (kontrolní zjištění č. 5) pak kontrolující dospěli k závěru, že výše uvedený rozsah osobních údajů odpovídá účelu, který kontrolovaný předmětným zpracováním osobních údajů sleduje. Kontrolou zároveň nebylo zjištěno, že by kontrolovaný prostřednictvím systému Face ID shromažďoval jiné osobní údaje.

S ohledem na uvedené kontrolující vyhodnotili rozsah údajů zpracovávaný kontrolovaným jako přiměřený účelu tohoto zpracování. Kontrolovaný tedy **neporušil** povinnost stanovenou v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679.

Kontrolní zjištění č. 7.

Kontrolující dále hodnotili, zda kontrolovaný v souvislosti s používáním Face ID zpracovává předmětné osobní údaje pouze po dobu nezbytnou pro účely tohoto zpracování, jak je jeho povinností dle čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679.

Doba uchování osobních údajů zpracovávaných v souvislosti s používáním Face ID je upravena v rámcové smlouvě a dokumentu „Technicko-organizační opatření k zabezpečení osobních údajů zpracovávaných v systému [redacted] (podklady č. 3.b a 3.c) následujícím způsobem:

<u>Serverová část</u>

Údaje zpracovávané v aplikaci jsou uloženy na serveru společnosti [redacted] po dobu 10 let, tj. po dobu trvání povinnosti vést stavební deník dle vyhlášky č. 499/2006 Sb. Oprávnění přistupovat k těmto údajům mají operátoři společnosti [redacted] a uživatelé (zaměstnanci kontrolovaného). Uživatelé mohou na tyto údaje nahlížet po dobu 6 měsíců od vrácení terminálu, po uplynutí této doby je třeba zažádat o přístup ze strany vedoucího pracovníka kontrolovaného. Kontrolovaný má dále možnost požádat společnost [redacted] o stažení údajů na médium a jejich výmaz ze serveru. Médium se staženými údaji je pak přiloženo ke stavebnímu deníku.

Terminál

Hash je v terminálu uložen obecně po dobu oprávnění vstupu daného pracovníka na stavbu, tj. zejména do ukončení stavby, skončení pracovního poměru či odnětí oprávnění na stavbu vstupovat. Uživatel nahlásí operátorovi společnosti [redacted] pracovníka, jehož hash požaduje z terminálu vymazat. Operátor následně zadá tento požadavek do aplikace, která se v řádech vteřin propojí s terminálem a dojde k výmazu hashe (viz také podklad č. 5).

Údaje o průchodech jsou v terminálu uchovávány maximálně po dobu 90 dní nebo po dosažení 150 000 průchodů, následně jsou z terminálu vymazány pro uvolnění paměti. Doba uchování tohoto údaje je tak závislá zejména na velikosti stavby a počtu zaměstnanců.

V případě ukončení stavby je terminál protokolárně vrácen a údaje v něm uložené zaměstnanci společnosti [redacted] neprodleně vymažou.

Shrnutí

Výše uvedené doby zpracování osobních údajů v jednotlivých zařízeních kontrolující hodnotí jako přiměřené účelu tohoto zpracování. Kontrolovaný tedy povinnost stanovenou v čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679 **neporušil**.

Kontrolní zjištění č. 8.

Další skupinou povinností, které se na kontrolovaného jako na správce osobních údajů vztahují, jsou povinnosti vyjádřené v čl. 12 až 14 nařízení (EU) 2016/679. Citovaná ustanovení upravují povinnost správce informovat subjekt údajů o všech podstatných parametrech zpracování osobních údajů, a to včetně jeho práv, která mu ve vztahu k tomuto zpracování vznikají (právo na přístup, právo požadovat vysvětlení, opravu či výmaz zpracovávaných údajů, popřípadě omezení jejich zpracování).

Kontrolou bylo zjištěno (podklady č. 3.l, 3.m, 4.a a 4.b), že informace o zpracování osobních údajů jsou všem pracovníkům poskytovány prostřednictvím informačních tabulí, které se nachází u vstupu na stavbu, v bezprostřední blízkosti terminálu. Tyto tabule obsahují informace v rozsahu:

- totožnost a kontaktní údaje správce,
- rozsah, ve kterém jsou osobní údaje zpracovávány,
- účel a doba zpracování,
- příjemci osobních údajů.

Na tabuli je dále informace o tom, že podrobnější informace o zpracování osobních údajů, zejména o právech subjektu údajů v souvislosti s tímto zpracováním, jsou zaměstnancům kontrolovaného přístupné v dokumentu „Informace o zpracování osobních údajů“ umístěném na intranetu kontrolovaného, a ostatním osobám (tj. zejména zaměstnancům subdodavatelů) na webových stránkách kontrolovaného, včetně odkazů na tyto dokumenty.

Kontrolou bylo ověřeno, že na webových stránkách kontrolovaného jsou informace o zpracování osobních údajů dostupné, a to v rozsahu (podklad č. 8):

- totožnost a kontaktní údaje správce,
- kategorie osobních údajů, jejich zdroje a účel zpracování,
- příjemci osobních údajů,
- práva subjektů údajů v souvislosti se zpracováním osobních údajů.

Kontrolující konstatují, že kontrolovaný **neporuši**l povinnosti stanovené v čl. 12 až 14 nařízení (EU) 2016/679.

Zároveň je však nutné konstatovat, že pro zvýšení transparentnosti v souladu se zásadou vyjádřenou v čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, která je mj. východiskem pro povinnosti upravené v čl. 12 a 13 a násl. tohoto nařízení, je na místě poskytované informace doplnit v tom smyslu, že prostřednictvím Face ID jsou zpracovávány biometrické údaje za účelem jednoznačné identifikace, přičemž tyto údaje spadají mezi zvláštní kategorie osobních údajů dle č. 9 nařízení (EU) 2016/679.

Kontrolní zjištění č. 9.

Další skupinou povinností, které se na kontrolovaného jako na správce osobních údajů vztahují, jsou povinnosti odpovídající právům subjektů údajů vyjádřeným čl. 15, 16, 17 a 21 nařízení (EU) 2016/679. Citovaná ustanovení upravují právo subjektů údajů na přístup k osobním údajům a právo požadovat jejich opravu či výmaz, případně vznést námitku proti zpracování těchto údajů.

Kontrolovaný dle svého vyjádření žádné výše uvedené žádosti dosud neeviduje (podklad č. 3). Postup pro jejich vyřizování je nicméně upraven v Organizačně řídící normě č. [redacted] Ochrana osobních údajů (podklad č. 7). Na základě tohoto dokumentu případné žádosti subjektů údajů vyřizuje zvláštní pověřenec pro ochranu osobních údajů za spolupráce dalších útvarů kontrolovaného. Zvláštní pověřenec zároveň vede evidenci přijatých opatření (omezení zpracování, výmaz, přenos osobních údajů aj.) v rozsahu identifikace příslušné databáze, kategorie osobních údajů a důvod předmětného omezení zpracování, výmazu či přenesení osobních údajů.

Kontrolou tak **nebylo zjištěno, že by kontrolovaný porušil** povinnosti odpovídající právům subjektů údajů upraveným v čl. 15, 16, 17 a 21 nařízení (EU) 2016/679.

Kontrolní zjištění č. 10.

Kontrolující dále hodnotili, zda kontrolovaný v souvislosti s používáním Face ID vede záznamy o činnostech zpracování, jak je jeho povinností dle čl. 30 odst. 1 nařízení (EU) 2016/679, který definuje i přesný obsah záznamů.

Kontrolovaný v souvislosti s používáním Face ID vede záznamy o činnostech zpracování (podklad č. 6.c). Obsahem těchto záznamů jsou údaje v rozsahu:
- kontaktní údaje správce osobních údajů (kontrolovaného),
- účely zpracování,

- příslušná organizačně řídící norma či právní předpis, na základě kterého je zpracování prováděno,
- právní titul zpracování,
- kategorie osobních údajů,
- kategorie subjektů údajů,
- kategorie příjemců osobních údajů,
- lhůty pro výmaz osobních údajů,
- údaje o případném předávání osobních údajů do třetích zemí,
- technická a organizační bezpečnostní opatření k ochraně osobních údajů.

Kontrolující konstatují, že kontrolovaný vede záznamy o činnostech, a to v požadovaném rozsahu. Povinnost stanovenou v čl. 30 odst. 1 nařízení (EU) 2016/679 tak kontrolovaný **neporušil**.

Také v této souvislosti je nicméně nutno upozornit, že záznamy o činnostech by měly odděleně zohlednit zpracování zvláštních kategorií osobních údajů, včetně přesné specifikace těchto údajů a odpovídajícího účelu zpracování.

Kontrolní zjištění č. 11.

Kontrolující dále hodnotili, zda a do jaké míry plní kontrolovaný v souvislosti s používáním Face ID povinnosti související se zabezpečením osobních údajů dle čl. 32 nařízení (EU) 2016/679.

Opatření k zabezpečení osobních údajů zpracovávaných prostřednictvím Face ID jsou upravena zejména v rámcové smlouvě (podklad č. 3.b), dokumentu Technicko-organizační opatření k zabezpečení osobních údajů zpracovávaných v systému [redacted] (podklad č. 3.c) a Organizačně řídící normě č. [redacted] Ochrana osobních údajů [redacted], podklad č. 7).

Z uvedených dokumentů a místních šetření vyplývají následující zjištění:

1. <u>Uchovávání údajů a jejich zabezpečení</u>

Údaje zpracovávané v aplikaci jsou ukládány na server umístěný v sídle společnosti [redacted]. Uvedené skutečnosti byly ověřeny při místním šetření v sídle společnosti [redacted] dne 28. listopadu 2018 (podklad č. 5).

Lokální síť, do které je zapojený server, je zabezpečena [redacted].

Komunikace mezi terminály a serverem probíhá [redacted]. Při každém průchodu terminál ukládá záznam o čase a směru průchodu a ID pracovníka. Údaje o průchodech jsou v [redacted] zasílány na server.

Vytvořený hash je uložen pouze v terminálu, na server není zasílán. [redacted]. Uložené hashe není možné přes menu terminálu zobrazit či s nimi jakkoli manipulovat. [redacted].

2. Zálohování

Serverová část systému je zálohována [redacted].

Údaje o docházce jsou zálohovány [redacted] kde zůstávají po dobu 60 dní. [redacted].

3. Přístupová oprávnění

Do serverové části mají přístup operátoři společnosti [redacted] a uživatelé – zaměstnanci kontrolovaného (viz podklady č. 3.d, 3.e a 3.g). Přístupová práva uživatelů do aplikace nastavuje operátor dle požadavku osoby oprávněné kontrolovaným (zpravidla vedoucí stavby). Přístupová práva jsou určována dle stromu kompetencí. Při vytvoření účtu uživatele [redacted] a přiděleno oprávnění k nahlížení do určené úrovně stromu kompetencí. [redacted].

Uživatel může nahlížet pouze na údaje těch pracovníků, kteří jsou zařazení pod jeho úrovní stromu. Každý uživatel může mít na stavbě pouze jeden uzel stromu jako vstupní bod. Uživatelé mají rovněž přístup k údajům o docházce. Rozsah zobrazených údajů pak závisí na vstupním bodu uživatele ve stromu kompetencí. Terminál (umístěný na stavbě) procházení docházkových údajů neumožňuje, tzn. na tyto údaje lze nahlížet pouze po přihlášení do aplikace. Přihlášení uživatele do aplikace probíhá [redacted]. Uživatelé komunikují pouze se serverem společnosti [redacted], dálková komunikace přímo s terminály není technicky možná. Přístup do administračního menu terminálu je zabezpečen [redacted] a umožňuje pouze změny v technickém nastavení terminálu.

4. Logování

Z přístupů operátorů a uživatelů do aplikace jsou pořizovány logy umožňující určit, kdo a kdy do aplikace přistupoval a na jaká data nahlížel (podklady č. 6.a a 6.b). Jednou týdně provádí administrátor kontrolu aplikace, jejíž součástí je mimo jiné kontrola logů, resp. kontrola

přístupů do aplikace. V rámci této kontroly by pak administrátor odhalil případný pokus o neoprávněný přístup.

V průběhu kontroly uzavřel kontrolovaný se společností [redacted] dodatek k rámcové smlouvě s účinností od 1. ledna 2019 (podklad č. 6.g). Na základě tohoto dodatku budou z kontrol aplikace pořizovány protokoly a společnost [redacted] bude kontrolovaného pravidelně (jednou měsíčně) informovat o výsledcích těchto kontrol.

5. Proškolování zaměstnanců

Zaměstnanci kontrolovaného, kteří z titulu své pracovní pozice přicházejí do styku s osobními údaji, obdrželi dokument „Pověření zaměstnance – osoby určené pro styk s osobními údaji“, jehož součástí je přehled povinností osoby určené pro styk s osobními údaji (podklad č. 3.f). Všichni zaměstnanci kontrolovaného jsou dále povinni znát obsah organizačně řídící dokumentace. Zaměstnanci byli opakovaně informováni o chystané účinnosti nařízení (EU) 2016/679 a s ní související novelou [redacted], a to jak formou školení vybraných zaměstnanců, tak písemně. [redacted] proběhla Technicko-ekonomická konference za účasti vrcholového managementu a vedoucích zaměstnanců kontrolovaného, kteří byli při této příležitosti seznámeni se základními principy ochrany osobních údajů. Po nabytí účinnosti nařízení (EU) 2016/679 dostali všichni zaměstnanci informační leták, jehož součástí byl mimo jiné odkaz na podrobné informace o zpracování osobních údajů na intranetu. [redacted] byla dle vyjádření kontrolovaného problematice ochrany osobních údajů rovněž věnována značná část novin kontrolovaného, které jsou dostupné všem zaměstnancům (podklad č. 3).

6. Povinnost mlčenlivosti

Povinnost mlčenlivosti zaměstnanců pověřených pro styk s osobními údaji je stanovena jak obecně v [redacted], tak v samotném dokumentu Pověření zaměstnance – osoby určené pro styk s osobními údaji, který daný zaměstnanec stvrzuje svým podpisem. Ve vztahu k operátorům (resp. všem zaměstnancům společnosti [redacted] povinnost mlčenlivosti vyplývá z čl. [redacted] a čl. [redacted] rámcové smlouvy (podklady č. 3.b, 3.f a 7).

Shrnutí

Kontrolující výše popsaná kontrolní zjištění shrnují konstatováním, že kontrolovaný **neporušil** povinnosti, které mu v souvislosti se zabezpečením osobních údajů vyplývají z čl. 32 nařízení (EU) 2016/679.

III. Poučení o opravném prostředku:

Proti kontrolnímu zjištění uvedenému v protokolu o kontrole může kontrolovaná osoba podat Úřadu pro ochranu osobních údajů ve lhůtě 15 dnů ode dne doručení protokolu o kontrole námitky.

Námitky se podávají písemně, musí z nich být zřejmé, proti jakému kontrolnímu zjištění směřují, a musí obsahovat odůvodnění nesouhlasu s tímto kontrolním zjištěním.

Pokud kontrolující inspektor nevyhoví námitkám ve lhůtě 7 dnů ode dne jejich doručení, vyřídí je předseda Úřadu pro ochranu osobních údajů ve lhůtě 30 dnů ode dne jejich doručení.

otisk
úředního
razítka

Mgr. et Mgr. Božena Čajková	inspektorka	.....
titul jméno příjmení	funkce	podpis
Mgr. Iva Tomášková	pověřený zaměstnanec Úřadu	.....
titul jméno příjmení	funkce	podpis
Josef Polák	pověřený zaměstnanec Úřadu	.....
titul jméno příjmení	funkce	podpis