



ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uouu.cz, www.uouu.cz



Čj. UOOU-02993/19-22
Praha 17. března 2020

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) (dále jen „nařízení (EU) 2016/679“) ve spojení s § 50 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů.

Kontrolující:

Mgr. et Mgr. Božena Čajková – inspektorka Úřadu, č. průkazu: [REDACTED] jako vedoucí kontrolní skupiny na základě pověření ke kontrole ze dne 3. prosince 2019;

Bc. Hana Imiolková – pověřená zaměstnankyně Úřadu, č. průkazu: [REDACTED], na základě pověření ke kontrole ze dne 3. prosince 2019;

Josef Polák – pověřený zaměstnanec Úřadu, č. průkazu: [REDACTED], na základě pověření ke kontrole ze dne 3. prosince 2019;

(dále jen „kontrolující“).

Kontrolovaná osoba:

[REDACTED] se sídlem [REDACTED], IČO: [REDACTED]
zastoupená [REDACTED] jednatelem, [REDACTED] generálním ředitelem

(dále jen „kontrolovaný“ nebo „[REDACTED]“).

Předmět kontroly:

Předmětem kontroly je dodržování povinností stanovených nařízením (EU) 2016/679 a zákonem č. 110/2019 Sb. v souvislosti se zpracováním osobních údajů zaměstnanců, zejména zákonnost zpracování, poskytování informací o zpracování a zabezpečení osobních údajů.

První kontrolní úkon:

Oznámení o zahájení kontroly čj. UOOU-02993/19-12, ze dne 05. prosince 2019.

Poslední kontrolní úkon:

Sdělení [REDAKCE] ze dne 06. března 2020, čj. UOOU-02993/19-21.

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. Podnět doručený Úřadu dne 21. června 2019, čj. UOOU-02993/19-1, počet listů 1, s přílohami:
 - 1.1. příloha – fotografie 1, počet listů 1;
 - 1.2. příloha – fotografie 2, počet listů 1;
2. Doplnění podání stěžovatelky ze dne 23.července 2019, čj. UOOU-02993/19-3, počet listů 1, s přílohami:
 - 2.1. příloha – [REDAKCE] souhlas, počet listů 1;
 - 2.2. příloha – [REDAKCE] souhlas, počet listů 1;
3. Sdělení stěžovatelky ze dne 16. srpna 2019, čj. UOOU-02993/19-6, počet listů 1;
4. Sdělení [REDAKCE] u ze dne 26. srpna 2019, čj. UOOU-02993/19-8, počet listů 2;
5. Oznámení o zahájení kontroly čj. UOOU-02993/19-12 ze dne 05. prosince 2019, počet listů 1, s přílohami:
 - 5.1. příloha – Pověření ke kontrole, počet listů 1;
6. Protokol o ústním jednání a místním šetření konaného dne 19. prosince 2019, čj. UOOU-02993/19-13, počet listů 4, s přílohami:
 - 6.1. příloha – Dotazník počet, listů 1;
 - 6.2. příloha – Protokol o kontrole z inspektorátu práce, počet listů 8;
7. Sdělení k Protokolu z ústního jednání a místního šetření ze dne 16. ledna 2020, čj. UOOU-02993/19-14, počet listů 5;
 - 7.1. příloha – Souhlas s použitím biometrických údajů za účelem evidence docházky, počet listů 11;
8. Sdělení k Protokolu z ústního jednání a místního šetření ze dne 22. ledna 2020, čj. UOOU-02993/19-16, počet listů 2;
 - 8.1. příloha – Dotazník 2, počet, listů 4;
9. Sdělení [REDAKCE] ze dne 26. února 2020, čj. UOOU-02993/19-19, počet listů 9;
10. Sdělení [REDAKCE] ze dne 06. března 2020, čj. UOOU-02993/19-21, počet listů 1;

10.1. příloha – [REDAKCE] souhlas, počet, listů 8;

10.2. příloha – [REDAKCE] souhlas, počet, listů 8.

V rámci kontroly je posuzováno výhradně zpracování osobních údajů v rozsahu stanoveném v předmětu kontroly a ledaže je níže uvedeno jinak, v čase provedení kontroly. Z výše uvedených podkladů jsou pro kontrolní zjištění v protokolu o kontrole výslovně vyhodnoceny pouze ty podklady, případně jejich části, v nichž jsou uvedeny relevantní informace.

II. Důvod kontroly:

Kontrola byla zahájena na základě podnětu doručeného Úřadu dne 21. června 2019. V podnětu bylo namítáno zpracování osobních údajů zaměstnanců v souvislosti s použitím docházkového systému (dále jen „DS“) s technologií umožňující rozpoznání otisků prstů, a sledování zaměstnanců prostřednictvím kamerového systému (dále jen „KS“), při práci s počítačem a pomocí GPS umístěných ve služebních vozích.

Zejména byla namítána zákonnost takového zpracování, poskytování informací o způsobu zpracování a zabezpečení osobních údajů.

Vzhledem k tomu, že některé výše uvedené skutečnosti již byly prověřovány Oblastním inspektorátem práce pro Jihomoravský a Zlínský kraj (dále jen „inspektorát“) (podklad č. 6.2.), zaměřili se kontrolující pouze na kontrolu plnění povinností [REDAKCE] u při zpracování osobních údajů zaměstnanců DS a KS.

III. Kontrolní zjištění:

Kontrolní zjištění č. 1:

- a) Kontrolující předně posuzovali, zda informace, které kontrolovaný v souvislosti s evidencí pracovní doby zpracovává, jsou osobními údaji ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679 nebo zvláštní kategorií osobních údajů podle čl. 9 bod 1 nařízení (EU) 2016/679. Podle čl. 4 bod 1 nařízení (EU) 2016/679 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*“ a zvláštní kategorie osobních údajů podle čl. 9 bod 1 nařízení (EU) 2016/679 pak představují 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*“.

Do zvláštní kategorie osobních údajů se dle čl. 9 bod 1 nařízení (EU) 2016/679 zahrnují také biometrické údaje, kterými se rozumí dle čl. 4 bod 14 nařízení (EU) 2016/679 „*osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických*

či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.“

██████████ používá u vstupních dveří do kanceláří zařízení pro identifikaci osob, tzv. docházkový terminál (dále jen „DT“), který umožňuje zaznamenat příchod a odchod jednotlivých zaměstnanců na základě technologie rozpoznání otisků prstů.

V DT jsou uloženy údaje o zaměstnancích v rozsahu jméno, příjmení, číslo přiřazené zaměstnanci DT, datum s časem příchodu a odchodu jednotlivých osob na pracoviště, záznam o počtu otisku prstů a otisk prstu zaměstnance převedený do číselné podoby (tzv. HASH kód, viz níže).

Data získaná snímáním otisků prstů zaměstnanců při příchodu na pracoviště nebo při odchodu z něj slouží k identifikaci dané osoby, jsou používána výhradně pro účely evidence pracovní doby v DS.

Pro identifikaci pomocí otisku prstu vybírá systém značky ██████████ z poskytnutého otisku některé rysy specifické pro jednotlivce (markanty). Na základě zjištěných markant pak vytváří biometrickou šablonu, kterou před uložením v systému zpracuje matematickou operací do číselného vyjádření (HASH kód). Takto vytvořený HASH kód (otisk prstu převedený do číselné podoby) je následně uložen v řídicí jednotce systému značky ██████████ zatímco obraz otisku prstu a zjištěné markanty jsou ihned po vytvoření HASH kódu mazány.

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 této právní regulace je nutno i využívání systémů pracujících s šablonami (tj. nikoli přímo s biometrickými údaji, ale jejich algoritmickým vyjádřením v podobě HASH kód) 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.

Kontrolovaný zpracovává biometrické údaje (otisk prstu převedený do číselné podoby) svých zaměstnanců, které umožňují jejich přímou identifikaci. Tento závěr lze dle kontrolujících přijmout s ohledem na dosavadní úroveň vědeckého poznání, dle kterého se má za to, že otisk prstu (a tím i z něj získaný HASH) je jedinečnou charakteristikou člověka, s jehož pomocí, bez potřeby dalších identifikátorů, lze provést spolehlivou identifikaci dané osoby.

Kontrolovaný prostřednictvím DS zpracovává identifikační údaje zaměstnanců včetně informace vypovídající o pracovní době, tedy osobní údaje ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, a zvláštní kategorie osobních údajů podle čl. 9 bod 1 nařízení (EU) 2016/679, konkrétně biometrické údaje ve smyslu čl. 4 bod 14 nařízení (EU) 2016/679.

- b) Dále kontrolující posuzovali, zda informace, které kontrolovaný zpracovává v souvislosti s instalovanými kamerami, jsou osobními údaji ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679.

Kontrolovaný provozuje ve svém firemním areálu na adrese [REDAKCE] [REDAKCE] KS se záznamem, který se skládá ze čtyř stacionárních kamer umístěných na vnějších pláštích budov. Kamery jsou namířeny na venkovní prostory – vstup do areálu, prostor mezi budovami a prostor parkoviště.

Monitorovací systém se záznamem umožňuje prohlížení záběrů z kamer, přičemž je zaznamenáván pouze obraz, bez zvukového záznamu.

Kontrolovaný je na pořízených záznamech schopen přímo identifikovat přinejmenším své zaměstnance. Ostatní zachycené osoby pak bude možné s pomocí pořízených záznamů identifikovat nepřímo, tj. na základě dalších informací dostupných buď kontrolovanému nebo příslušným orgánům (např. orgánům činným v trestním řízení), (podklad č. 7).

Obsahem pořízených záznamů jsou tedy informace vypovídající o jednání osob v monitorovaných prostorech, které lze (přinejmenším v případě zaměstnanců) přiřadit ke konkrétním fyzickým osobám.

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

Kontrolní zjištění č. 2:

Dále kontrolující hodnotili, zda jsou uvedené osobní údaje DS a KS zpracovávány ve smyslu čl. 4 bod 2 nařízení (EU) 2016/679, podle kterého „*je zpracováním osobních údajů jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů.*“ a současně posuzovali 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.*“

- a. DS byl rozhodnutím vedení firmy [REDAKCE] zřízen za účelem splnění zákonem stanovené povinnosti. Kontrolovaný jako zaměstnavatel má dle zvláštního právního předpisu, zákona č. 262/2006 Sb., zákoník práce, povinnost vést evidenci pracovní doby zaměstnanců. V této souvislosti jsou v DT shromažďovány a dále uchovávány výše uvedené osobní údaje, s nimiž [REDAKCE] provádí soubor operací ve smyslu čl. 4 bod 2 nařízení (EU) 2016/679. (podklad č. 6)
- b. Na základě rozhodnutí vedení, kontrolovaný v areálu firmy instaloval a provozuje KS se záznamem, který umožňuje automatizované monitorování prostoru, prostřednictvím kterého dochází ke shromažďování, zaznamenávání, ukládání na nosič informací, jeho uchovávání po určitou dobu a likvidaci. V případě incidentu zpřístupní kamerový záznam

s osobními údaji Policii ČR. Účelem tohoto rozhodnutí bylo zajistit ochranu majetku a bezpečí osob na pracovišti. (podklad č. 6).

Operace, respektive soubor operací, které jsou u kontrolovaného prováděny s osobními údaji v DS a KS, jsou nepochybně zpracováním osobních údajů, proto kontrolující na základě výše uvedeného konstatují, že [REDAKCE] **zpracovává** osobní údaje ve smyslu čl. 4 bod 2 nařízení (EU) 2016/679.

Kontrolující s ohledem na výše uvedené konstatují, že [REDAKCE] je v postavení **správce** podle čl. 4 bodu 7 nařízení (EU) 2016/679, neboť určil účel, způsob a prostředky předmětného zpracování osobních údajů.

Kontrolující dále prověřili skutečnosti (namítané v podnětu), ohledně kamer umístěných na stojanu v areálu firmy. De tvrzení stěžovatele kamery snímaly také prostor mimo firmu kontrolovaného. Z fotodokumentace (podklad č. 1.1, 1.2.) je patrné jejich umístění u zadní části kancelářské budovy a jejich nasměrování k vjezdu do areálu. Uvedené kamery jsou ve vlastnictví nájemce ([REDAKCE]), který se zabývá prodejem KS, jejichž funkce a možnosti předváděl svým zákazníkům. Jedna z kamer sloužila k prezentaci snímání státní poznávací značky a další k panoramatickým záběrům.

V době kontroly byl stojan s kamerami přemístěn do jiné části areálu (podklad č. 6.2.). Vzhledem k tomu, že z těchto kamer nebyl a není pořizován žádný záznam, nedochází ke zpracování osobních údajů ve smyslu čl. 4 bod 1 a 2 nařízení (EU) 2016/679.

Kontrolní zjištění č. 3:

Kontrolující se dále zabývali skutečností, zda zpracování osobních údajů, které je předmětem této kontroly, probíhá v souladu s čl. 6 a čl. 9 nařízení (EU) 2016/679, podle kterého musí správce osobních údajů vždy disponovat legitimním právním titulem.

Podle čl. 6 odst. 1 nařízení (EU) 2016/679 *zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:*

- a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
- b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
- c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
- d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
- e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
- f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

Podle ustanovení článku 9 odst. 1 nařízení (EU) 2016/679 se „zakazuje zpracování osobních údajů, které vypovídají 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“.

Podle odstavce 2 uvedeného článku se odstavec 1 nepoužije, pokud jde o některý z případů, uvedených v písmenech a) až j) tohoto odstavce.

Odstavec 1 se nepoužije, pokud:

„subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz uvedený v odst. 1 nemůže být subjektem údajů zrušen.“

- a. Kontrolující hodnotili, zda kontrolovaný disponuje právním titulem pro zpracování osobních údajů, včetně zvláštních kategorií osobních údajů zaměstnanců, v souvislosti s používáním DS založeném na principu snímání otisků prstů, 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 některým z obecných právních titulů i právním titulem pro zpracování zvláštních kategorií údajů.

Jak již bylo výše popsáno (viz kontrolní zjištění č. 1 a 2), kontrolovaný pro evidenci pracovní doby používá u vstupních dveří do kanceláří zařízení DT, který umožňuje zaznamenat příchod a odchod jednotlivých zaměstnanců pomocí identifikace na základě technologie rozpoznání otisků prstů za účelem plnění povinnosti stanovené zvláštním právním předpisem. Konkrétně se jedná o povinnost vést evidenci pracovní doby zaměstnanců podle § 96 zákona č. 262/2006 Sb., zákoník práce.

Pro zpracování osobních údajů zaměstnanců, které jsou uloženy v DT v rozsahu jméno, příjmení, číslo přiřazené zaměstnanci DT, časový údaj o příchodu a odchodu z pracoviště, je dán právní titul dle čl. 6 bod 1 písm. c) nařízení (EU) 2016/679, podle kterého je zpracování „zákonné, pokud je nezbytné pro splnění právní povinnosti, která se na správce vztahuje“.

Kontrolou nebylo zjištěno, že by zpracování těchto osobních údajů bylo v rozporu se zákoníkem práce, kontrolovaný tak povinnost vyplývající z čl. 6 bod 1 písm. c) nařízení (EU) 2016/679 **neporušil**.

██████████ za účelem vedení evidence pracovní doby zpracovává i zvláštní kategorii osobních údajů. Zpracování biometrických údajů v DT (HASH – markanta z otisku prstu převedená do číselné podoby) kontrolovaný provádí na základě výslovného souhlasu subjektů údajů.

Kontrolovanému udělilo souhlas celkem 7 zaměstnanců z 8, a to podpisem dokumentu Souhlas se zpracováním osobních a biometrických údajů a poučení subjektu údajů (dále jen „souhlas I“ nebo „dokument I“) (podklad č. 2.1.a 2.2.).

V dokumentu I byl zaměstnanci udělen jediný souhlas se zpracováním v něm uvedených osobních údajů pro různé účely. Jméno a příjmení, adresu, e-mail, telefonní číslo, datum narození, zdravotní stav/omezení a údaje o zdravotní pojišťovně pro vnitrofiremní záležitosti, účetní a daňové účely, obrazové a zvukové záznamy prostřednictvím KS za účelem zabezpečení majetku, biometrický otisk prstu pro účely evidence docházky, a zpracování lokalizačních údajů za účelem evidence knihy jízd.

Kontrolující se nezabývali hodnocením souhlasu pro všechny v něm stanovené účely, neboť ke zpracování osobních údajů zaměstnanců v souvislosti s pracovním poměrem a s ním souvisejících povinností kontrolovaného jako zaměstnavatele, není takového souhlasu třeba a je považován za nadbytečný.

Vzhledem k výše uvedenému byly kontrolujícími hodnoceny náležitosti souhlasu pouze z hlediska zpracování biometrických údajů zaměstnanců pro vedení evidence pracovní doby DS.

Souhlas I obsahoval informace:

- o osobě správce (kontrolovaném);
- o osobách, kterým mohou být zpracovávány osobní údaje zpřístupněny pro účetní a daňové účely;
- o dobrovolnosti poskytnutí osobních i biometrických údajů,
- o době uchování záznamů KS;
- poučení o jejich právu na informace o zpracování osobních údajů a přístupu k těmto údajům; právu kdykoliv souhlas odvolat; právu na omezení zpracování údajů; právu na výmaz.

Požadavky na souhlas se zpracováním osobních údajů jsou v nařízení (EU) 2016/679 vyjádřeny v čl. 4 bod 11, podle kterého je souhlas „*subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů*“ a v čl. 7 nařízení (EU) 2016/679, kde jsou stanoveny podmínky vyjádření souhlasu, ze kterých vyplývá zejména, že:

1. správce musí být schopen doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů;
2. souhlas subjektu údajů musí být srozumitelný;
3. subjekt údajů má právo svůj souhlas kdykoli odvolat. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně snadné jako jej poskytnout.

Souhlas udělený v dokumentu I nesplňoval zákonné požadavky, neboť:

- neumožňoval jednoznačně udělit či neudělit souhlas za účelem evidence pracovní doby;
- nenabízel možnost výběru alternativy v případě vyjádření nesouhlasu s poskytnutím biometrických údajů;
- nezahrnoval informace o způsobu jejich zpracování;
- nesplňoval požadavky na informační povinnost správce dle čl. 12 v rozsahu informace dle čl. 13 nařízení (EU) 2016/679 (viz kontrolní zjištění č. 4).

Jelikož HASH kód je považován za biometrický údaj, je nezbytné při takovém zpracování brát v potaz čl. 9 odst. 1 nařízení (EU) 2016/679, který zakazuje zpracování biometrických údajů. V čl. 9 odst. 2 nařízení (EU) 2016/679 jsou pak stanoveny z tohoto zákazu výjimky, v daném případě je zpracování možné jen na základě právního titulu dle čl. 9 odst. 2 písm. a) nařízení (EU) 2016/679, tedy pokud subjekt údajů udělil výslovný souhlas se zpracováním zvláštní kategorie osobních údajů.

Udělený souhlas I nespĺňoval zákonné požadavky, neboť informace a poučení subjektu údajů o účelu, způsobech a době zpracování biometrického údaje (otisku prstu) nebylo zcela jednoznačně formulováno, nebylo transparentní. Kontrolující na základě uvedeného dospěli k závěru, že kontrolovaný nedisponuje výslovným souhlasem se zpracováním otisku prstu dle čl. 9 odst. 2 písm. a), porušil tak povinnost zákonného zpracování podle čl. 9 nařízení (EU) 2016/679.

V průběhu kontroly došlo k uvedení souhlasu do souladu s nařízením (EU) 2016/679, kontrolovaný upravil jeho náležitosti a vše doložil dokumentem Souhlas s použitím biometrických údajů za účelem evidence docházky (dále jen „souhlas II“) (podklad č. 7.1.) v němž:

- *byl upraven rozsah osobních údajů, kterých se souhlas týká (jméno a příjmení, datum narození, adresa a samotný biometrický údaj – HASH kód);*
- *jednoznačně byla dána možnost udělit či neudělit souhlas formou zaškrtnutých polí (uděluji, neuděluji) a vlastnoručním podpisem;*
- *byla doplněna informace, že v případě neudělení souhlasu s použitím biometrického údaje, bude subjektu údajů vytvořena osobní čipová karta;*
- *do souhlasu II byly také včleněny informace o podmínkách a způsobu zpracování;*
- *doplněna informační povinnost dle čl. 12 a čl. 13 nařízení (EU) 2016/679, viz kontrolní zjištění č. 4.*
- *byla doplněna informace o době uchování záznamů otisků prstů (po dobu trvání souhlasu II, nebo do ukončení pracovního poměru zaměstnance).*

Kontrolovanému udělilo výslovný souhlas II celkem 8 zaměstnanců z 8.

K výše uvedenému lze uvést, že 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 situaci, kdy je subjekt údajů v podřízeném postavení vůči správci osobních údajů (vztah zaměstnanec – zaměstnavatel), je při hodnocení platnosti souhlasu obzvláště nutné dbát na dodržení prvku dobrovolnosti a svobody tohoto právního úkonu. V případě, kdy by se neudělení souhlasu mohlo jakkoli promítnout do pracovníprávního vztahu zaměstnance, nelze požadavky na souhlas se zpracováním osobních údajů považovat za splněné. Uvedené platí obzvláště v situaci, kdy předmětné zpracování osobních údajů zcela zjevně není ve prospěch zaměstnanců.

- b. Kontrolující se dále zabývali zákonností zpracování osobních údajů v souvislosti s provozovaným KS v areálu objektu dle čl. 6 bod 1 písm. f) nařízení (EU) 2016/679, podle kterého je *„zpracování nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů.“*

Za účelem ochrany majetku a bezpečí na pracovišti je možné prostřednictvím KS se záznamem zpracovávat osobní údaje zaměstnanců, případně dalších osob, na základě oprávněných zájmů správce dle čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679.

Pořízení kamerového záznamu podle ustanovení čl. 6 bod 1 písm. f) nařízení (EU) 2016/679 předpokládá, že je monitorován především majetek firmy, případně veřejnosti (zákazníků, externích dodavatelů) a z části i pohyb osob (veřejnosti a zaměstnanců) v těchto provozních prostorech firmy.

Proti neoprávněnému zpracování svých osobních údajů požívají zaměstnanci navíc ochrany podle § 316 odst. 2 zákona č. 262/2006 Sb., zákoníku práce, kdy *„zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.“*

Kamery v areálu kontrolovaného nezabírají prostor pracoviště zaměstnanců, nemonitorují tedy pracoviště jednotlivých zaměstnanců, ani nesledují zaměstnance při práci, a to ani za účelem sledování jejich pracovní výkonnosti apod. (podklad č. 6)

Kontrolující vyhodnotili zjištěný stav tak, že kontrolovaný **neporušil** povinnost stanovenou v čl. 6 odst. 1 písm. f), tedy že zpracování osobních údajů zaměstnanců prostřednictvím KS lze hodnotit jako nezbytné pro plnění oprávněných zájmů správce.

Kontrolní zjištění č. 4:

Kontrolující hodnotili rovněž plnění povinnosti uvedené v ustanovení čl. 12 nařízení (EU) 2016/679, v souvislosti s poskytováním informací, v rozsahu čl. 13 tohoto nařízení. Uvedená 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.

Podle čl. 12 nařízení (EU) 2016/679 *„správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v čl. 13 nařízení (EU) 2016/679.“*

Podle čl. 13 nařízení (EU) 2016/679 správce je při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být

osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Povinnost dle citovaného zákonného ustanovení je povinen správce splnit před zpracováním osobních údajů subjektů údajů.

O instalaci DS a jeho způsobu používání byli zaměstnanci vyrozuměni ústně na firemní poradě. A začátkem roku 2019 byli informováni o KS. Podle zjištění oblastního inspektorátu práce měli být zaměstnanci informováni pouze o umístění jednotlivých kamer, a ne o rozsahu kontroly a způsobech jejího provádění prostřednictvím KS. Na základě kontroly inspektorátu byli zaměstnanci dodatečně informováni také o rozsahu kontroly a způsobech jejího provádění. (podklad č. 6.2.)

Další informace k DS a KS byly součástí souhlasu I. (podklady č. 2.1., 8, 9) (viz kontrolní zjištění č. 2):

- totožnost a kontaktní údaje správce;
- účely a rozsah osobních údajů, které jsou zpracovávány;
- prostředky zpracování osobních údajů;
- osoby, kterým mohou být zpracovávány osobní údaje zpřístupněny;
- o dobrovolnosti poskytnutí osobních i biometrických údajů;
- práva subjektů údajů v souvislosti se zpracováním osobních údajů.

Informační povinnost nesplňovala veškeré zákonné náležitosti tak, jak jsou uvedeny v čl. 13 nařízení (EU) 2016/679, neboť zaměstnanci nebyli informováni o způsobu a podmínkách zpracování osobních údajů v DS a možném přístupu osob k těmto údajům.

Vzhledem k tomu, že poskytnuté informace ohledně předmětného zpracování osobních údajů, nesplňovaly všechny podstatné parametry stanovené v čl. 12 nařízení (EU) 2016/679, v rozsahu informace podle čl. 13 nařízení (EU) 2016/679, kontrolující vyhodnotili zjištěný stav tak, že kontrolovaný **porušil** povinnost stanovenou v čl. 12 nařízení (EU) 2016/679.

Správce na základě zjištění kontrolujících v dokumentu souhlas II přepracoval informační povinnost (podklad č. 7.1.) podle požadavků výše uvedených článků nařízení (EU) 2016/679 (došlo k upřesnění informací o způsobech a podmínkách zpracování osobních údajů, jejich zabezpečení a přístupu k údajům v DS).

Kontrolní zjištění č. 5:

Kontrolující rovněž zjišťovali, zda a do jaké míry kontrolovaný plní povinnosti týkající se zabezpečení osobních údajů v souvislosti s předmětem kontroly, jak je jeho povinností podle čl. 25 a čl. 32 nařízení (EU) 2016/679.

a) Posouzení úrovně zabezpečení zpracovávaných osobních údajů DS:

Kontrolovaný používá u vstupních dveří do kanceláří zařízení značky ████████ model ████████ určené jako DT, který umožňuje zaznamenat příchod a odchod jednotlivých zaměstnanců pomocí identifikace na základě technologie rozpoznání otisků prstů. DT je čtecí (skenovací) jednotka značky ████████, která pracuje v režimu off-line.

V DT jsou uloženy údaje v rozsahu základních identifikačních údajů zaměstnance a číslo jemu přiřazené DT, záznam o počtu otisku prstů a otisk prstu převedený do číselné podoby (tzv. HASH kód, viz níže) a informace o datu, čase příchodu a odchodu z pracoviště.

Pro identifikaci pomocí otisku prstu vybírá DT z poskytnutého otisku některé rysy specifické pro jednotlivce (markanty). Na základě zjištěných markantů pak vytváří biometrickou šablonu, kterou před uložením v systému zpracuje matematickou operací do číselného vyjádření (HASH kód). Takto vytvořený HASH kód (otisk prstu převedený do číselné podoby) je následně uložen v řídicí jednotce systému značky [REDACTED], zatímco obraz otisku prstu a zjištěné markanty jsou ihned po vytvoření HASHe mazány.

Do DT má přístup pouze vedení kontrolovaného v pozici administrátora (podklad č. 6). Data z něj jsou vyhodnocena měsíčně za účelem splnění zákonem stanovené povinnosti, evidence pracovní doby zaměstnance. [REDACTED]

Informace o datu a čase příchodu a odchodu ze zaměstnání jsou uchovávány po dobu stanovenou zvláštním právním předpisem (pro účetní a daňové účely). Data z DT jsou vyhodnocena měsíčně za účelem splnění zákonem stanovené povinnosti, evidence pracovní doby zaměstnance. [REDACTED]

Veškeré osobní údaje jsou v terminálu uchovávány jen po dobu trvání souhlasu nebo do ukončení pracovního poměru zaměstnance, jsou chráněny šifrováním, které je nastavené výrobcem DS jednotky. DT, není připojen do žádné sítě ani k serveru. Pomine-li právní titul pro zpracování osobních údajů zaměstnance, jsou vedením firmy v DS neprodleně smazány.

Postup spočívající ve vytvoření a následném využívání HASH biometrického údaje v DS pak lze považovat za jeden z prvků zabezpečení.

b) Posouzení úrovně zabezpečení zpracovávaných osobních údajů KS:

Kontrolovaný provozuje ve svém firemním areálu na adrese [REDACTED] KS se záznamem, který se skládá ze čtyř stacionárních kamer umístěných na vnějších pláštích budov. Kamery jsou namířeny na venkovní prostory: vstup do areálu, prostor mezi budovami a prostor parkoviště, dochází k automatizovanému záznamu obrazu monitorovaného prostoru, nikoliv záznamu zvuku.

Záznamové zařízení je chráněno přístupovým heslem s vnitřním šifrováním. (podklad č. 7)

[REDACTED]

Do monitorovacího informačního systému má přístup jeden uživatel. Tento uživatelský účet je sdílen. Znalost hesla a s tím i možnost pracovat se záznamy mají dvě osoby. V režimu on-line lze sledovat záběry ze všech kamer jednotlivě nebo současně, zaznamenávají pouze video signál.

Dohledový software umožňuje on-line sledování všech kamer i vyhledávání záběru z historie záznamů. Záznamy jsou uloženy po dobu sedmi dnů. K odmazávání starých záznamů dochází automaticky. Logování činností tento systém umožňuje. Auditní stopa o tom, k čemu a kdy došlo v aplikaci, je zaznamenána.

Přístup do kanceláře má omezený počet osob. Logování činností dohledového systému je zapnuto.

Záznam je ukládán z kamer do záznamového zařízení ve formátu *.dav, tj. proporcionální formát výrobce, firmy ██████████. Soubor se nachází pouze v paměti záznamového zařízení a je standardní cestou nepřístupný. Samotné záznamové zařízení je přístupné pouze vedení společnosti jak fyzicky, tak programově.

Zařízení monitoruje kompletní logování (uživatelské jméno, čas připojení a informaci o tom co se sleduje na záznamu) a je chráněno přístupovým heslem s vnitřním proporcionálním systémem uložení dat. Záznam z KS není dále předáván. Slouží pouze jako bezpečnostní opatření majetku firmy.

K tomu lze obecně uvést, že celý objekt je oplocen, vstup do objektu je přes uzavíratelnou bránu, vnitřní prostory jsou zabezpečeny i pohybovými senzory a vše je napojeno na bezpečnostní službu.

Na základě výše uvedených skutečností dospěli kontrolující k závěru, že kontrolovaný plní povinnosti dle čl. 25 a čl. 32 nařízení (EU) 2016/679, **porušení nebylo shledáno**.

IV. 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.

Podpisová doložka:

otisk
úředního
razítka

Mgr. et Mgr. Božena Čajková	inspektorka Úřadu	<u>(podepsáno elektronicky)</u> podpis
Bc. Hana Imiolková	pověřená zaměstnankyně Úřadu	<u>(podepsáno elektronicky)</u> podpis
Josef Polák	pověřený zaměstnanec Úřadu	<u>(podepsáno elektronicky)</u> podpis