



ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

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



Čj. UOOU-04332/23-30
Praha 13. listopadu 2024

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. Marek Šnajdr – pověřený zaměstnanec Úřadu, č. průkazu: [REDACTED], jako vedoucí kontrolní skupiny na základě pověření ke kontrole ze dne ze dne 12. prosince 2023,

Mgr. Jaromír Kuba – pověřený zaměstnanec Úřadu, os. č. [REDACTED], na základě pověření ke kontrole ze dne ze dne 12. prosince 2023,

a

Bc. Šárka Hozmanová – pověřená zaměstnankyně Úřadu, č. průkazu: [REDACTED], na základě pověření ke kontrole ze dne 12. prosince 2023.

Kontrolovaná osoba:

[REDACTED]
(dále jen „kontrolovaná osoba“).

Předmět kontroly:

Dodržování povinností stanovených nařízením (EU) 2016/679 a zákonem č. 110/2019 Sb. ve znění pozdějších předpisů v souvislosti se zpracováním osobních údajů v rámci docházkového či obdobného systému využívaného kontrolovanou osobou.

První kontrolní úkon:

Oznámení o zahájení kontroly, čj. UOOU-04332/23-6, které bylo doručeno kontrolované osobě 19. prosince 2023.

Poslední kontrolní úkon:

Zpracování *Úředního záznamu o pořízení dokumentace* ze dne 5. listopadu 2024, čj. UOOU-04332/23-29.

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. *Vyjádření ke kontrole dle § 3 zákona č. 255/2012 Sb* ze dne 15. září 2023, čj. UOOU-04332/23-3, počet listů 4;
2. *Oznámení o zahájení kontroly* ze dne 19. prosince 2023, čj. UOOU-04332/23-6, počet listů 2;
3. *Vyjádření k Žádosti o součinnost* ze dne 24. ledna 2024, čj. UOOU-04332/23-10, počet listů 2;
4. *Vyjádření ke kontrole dle § 3 zákona č. 255/2012 Sb* ze dne 30. ledna 2024, čj. UOOU-04332/23-11, počet listů 7;
5. *Odpověď povinné osoby na žádost o součinnost* ze dne 20. března 2024, čj. UOOU-04332/23-16, počet listů 1;
6. *Protokol z ústního jednání a místního šetření* (povinná osoba) ze dne 21. března 2024, čj. UOOU-04332/23-17, počet listů 2,
 - 6.1. příloha č. 1 – snímky obrazovky (systém , počet listů 5;
7. *Protokol z ústního jednání a místního šetření* (kontrolovaná osoba) ze dne 21. března 2024, čj. UOOU-04332/23-18, počet listů 2,
 - 7.1. příloha č. 1 – fotografie docházkových hodin, počet listů 1,
 - 7.2. příloha č. 2 – fotografie docházkového systému, počet listů 3;
8. *Vyjádření ke kontrole* ze dne 26. března 2024, čj. UOOU-04332/23-19, počet listů 1.
9. *Vyjádření ke kontrole* ze dne 19. srpna 2024, čj. UOOU-04332/23-21, počet listů 1.
10. *Vyjádření ke kontrole* ze dne 5. září 2024, čj. UOOU-04332/23-23, počet listů 1.
11. *Vyjádření povinné osoby* ze dne 19. září 2024, čj. UOOU-04332/23-25, počet listů 1.
12. *Úřední záznam o pořízení dokumentace* ze dne 9. října 2024, čj. UOOU-04332/23-26, počet listů 1,

12.1. příloha č. 1 – VŠEOBECNÉ OBCHODNÍ PODMÍNKY UŽÍVÁNÍ SYSTÉMU [REDAKCE]
platné a účinné od [REDAKCE] číslo verze: [REDAKCE], počet listů 2.

13. Vyjádření ke kontrole ze dne 30. října 2024, čj. UOOU-04332/23-28, počet listů 1.

14. Úřední záznam o pořízení dokumentace ze dne 5. listopadu 2024, čj. UOOU-04332/23-29, počet listů 1.

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 kontrolního plánu Úřadu pro rok 2023.

III. Kontrolní zjištění:

Veřejně dostupné informace o kontrolované osobě:

Dle Výpisu z obchodního rejstříku je kontrolovaná osoba společností s ručením omezeným, IČO: [REDAKCE], s datem vzniku a zápisu [REDAKCE], spisová značka [REDAKCE] vedená u [REDAKCE]. Předmětem podnikání je „Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona“ v oborech činnosti „Vydavatelské činnosti, polygrafická výroba, knihařské a kopírovací práce“, „Výroba školních a kancelářských potřeb, kromě výrobků z papíru, výroba bižuterie, kartáčnického a konfekčního zboží, deštníků, upomínkových předmětů“, „Zprostředkování obchodu a služeb“, „Velkoobchod a maloobchod“, „Skladování, balení zboží, manipulace s nákladem a technické činnosti v dopravě“, „Nákup, prodej, správa a údržba nemovitostí“, „Příprava a vypracování technických návrhů, grafické a kresličské práce“, „Reklamní činnost, marketing, mediální zastoupení“ a „Návrhářská, designérská, aranžérská činnost a modeling“.

Kontrolovaná osoba provozuje webové stránky [REDAKCE]. Zde svou činnost prezentuje jako velkoobchod s papírenským zbožím, především školními a kancelářskými potřebami, pohlednicemi, přáními do obálky, balicími papíry, omalovánkami a kalendáři (bod 14.1 přehledu podkladů, str. 2).

Kontrolní zjištění č. 1

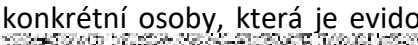
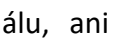
Kontrolovaná osoba od měsíce dubna roku 2022 (bod 10 přehledu podkladů, str. 1) do data vydání tohoto protokolu využívá za účelem evidence docházky zaměstnanců elektronický systém, jehož dodavatelem je [REDAKCE] (bod 1 přehledu podkladů, str. 2, dále jen [REDAKCE]). Evidence docházky probíhá prostřednictvím přiložení libovolného prstu k docházkovému terminálu, nebo přiložením [REDAKCE] čipu. Všichni zaměstnanci kontrolované osoby mají k dispozici vlastní [REDAKCE] čip. Buď jako jediný způsob

evidence docházky, nebo, v případě udělení souhlasu s využitím otisků prstů, jako jednu ze dvou alternativ zaznamenání docházky.

V docházkovém systému jsou vedeny údaje zaměstnanců v celkovém rozsahu jméno, příjmení, telefonní číslo, emailová adresa, hashe otisků prstů, číslo bankovního účtu (bod 6 přehledu podkladů, str. 2), začátek a konec pracovního poměru, týdenní pracovní doba, rodné číslo, typ pracovního úvazku, pozice, docházkový pin, adresa, časy příchodů a odchodů do/ze zaměstnání, odpracované hodiny a fotografie (bod 6 přehledu podkladů). Každý zaměstnanec má přístup do svého profilu v systému a může si libovolně doplnit údaje (bod 7 přehledu podkladů, str. 2). Vždy jsou vyplněny údaje pouze v rozsahu jméno, příjmení, začátek pracovního poměru, týdenní pracovní doba, emailová adresa, typ pracovního úvazku a údaje o docházce zaměstnance (bod 6.1 přehledu podkladů, str. 3).

Kontrolovaná osoba nakládá s údaji, které splňují definici osobních údajů podle čl. 4 bodu 1 nařízení (EU) 2016/679, a to způsobem odpovídajícím definici zpracování osobních údajů podle čl. 4 bodu 2 nařízení (EU) 2016/679.

Kontrolní zjištění č. 2

Docházkový terminál převádí při prvotním přiložení otisk prstu na tzv. hash kód (konkrétně se jedná o „seznam a vlastnosti významných znaků - markantů v otisku prstu“ dle normy , který je uložen do systému  a z něj nelze zpětně obnovit původní podobu otisku prstů. Při následném přiložení prstu za účelem evidence docházky provádí jeho vyhodnocení a porovnání s již existujícími hash kódy v databázi všech uložených markantů ostatních otisků . Na základě vyhodnocení shod je v systému poskytnuta informace o příchodu či odchodu konkrétní osoby, která je evidována v systému. Databáze je uložena v  a také se synchronizuje do jednotlivých terminálů (v zabezpečené části paměti aplikace, do které nemá kontrolovaná osoba přístup, markanty nelze vyexportovat ani z terminálu, ani z ). Terminály komunikují s  pomocí  zabezpečeného pomocí HTTPS a dále s několika sadami komunikačních klíčů (bod 3 přehledu podkladů, str. 1).

Samotný hash kód je tedy unikátní pro každého zaměstnance kontrolované osoby a vyjadřuje v číselné podobě fyzické znaky tohoto zaměstnance. Pomocí hash kódu je zaměstnanec identifikován pro účel zaznamenání docházky (porovnáním s ostatními hash kódy v databázi ).

V případě hash kódů otisků prstů zaměstnanců nakládá kontrolovaná osoba s údaji, které splňují definici biometrických údajů podle čl. 4 bodu 14 nařízení (EU) 2016/679. Jedná se o zpracování zvláštních kategorií osobních údajů dle čl. 9 nařízení (EU) 2016/679.

Kontrolní zjištění č. 3

 na základě odsouhlasení *Všeobecných obchodních podmínek užívání systému*  (bod 12, příloha 1 přehledu podkladů) kontrolovanou osobou poskytuje kontrolované osobě softwarovou službu ve formě aplikace, jejíž *Modul docházka*

využívaný kontrolovanou osobou slouží k evidenci docházky zaměstnanců, a dále též příslušný hardware, tzv. píchací hodiny.

Kontrolovaná osoba určila předmět a prostředky zpracování (evidence docházky zaměstnanců pomocí docházkového systému [REDAKCE], což odpovídá postavení správce osobních údajů.

[REDAKCE] na základě pokynů správce (kontrolované osoby) zpracovává osobní údaje zaměstnanců (rozsah uveden výše) kontrolované osoby. Výstupem zpracování jsou informace o docházce jednotlivých zaměstnanců kontrolované osoby. Toto odpovídá postavení zpracovatele osobních údajů.

Smlouva mezi kontrolovanou osobou a [REDAKCE] byla uzavřena elektronicky aktivací přístupu do administračního rozhraní docházkového systému [REDAKCE] kontrolované osobě, k němuž došlo v měsíci dubnu roku 2022 (bod 10 přehledu podkladů, str. 1). Ve *Všeobecných obchodních podmínkách užívání systému* [REDAKCE] je v souladu s výše uvedeným [REDAKCE] postavena do role zpracovatele osobních údajů, která se řídí pokyny kontrolované osoby jako objednatele systému.

Od dubna roku 2022 do data vydání tohoto protokolu byly do docházkového systému využívaného kontrolovanou osobou zavedeny hashe otisků prstů nejméně 57 zaměstnanců kontrolované osoby (bod 9 přehledu podkladů, bod 1).

Kontrolovaná osoba je v postavení správce osobních ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679. [REDAKCE] je v postavení zpracovatele osobních údajů ve smyslu čl. 4 bodu 8 nařízení (EU) 2016/679.

Kontrolní zjištění č. 4

Kontrolovaná osoba pro účel evidence docházky zaměstnanců zpracovává osobní údaje standardně v rozsahu jméno, příjmení, začátek a konec pracovní smlouvy, [REDAKCE] čip (bod 7 přehledu podkladů, str. 2), přičemž další údaje si zaměstnanci do docházkového systému mohou vložit podle své vlastní vůle (bod 3 přehledu podkladů, str. 3). Zpracování probíhá na základě právních základů dle čl. 6 odst. 1 písm. b) a c) nařízení (EU) 2016/679, s výjimkou biometrických údajů, pro které kontrolovaná osoba využívá výjimku dle čl. 9 odst. 2 písm. a) nařízení (EU) 2016/679, tedy výslovný souhlas subjektu údajů (bod 13 přehledu podkladů, str. 1).

V případě udělení souhlasu se zpracováním otisku prstů zaměstnancem kontrolované osoby je dále zpracován hash otisku prstu (souhlas je udělen podpisem *Souhlasu se zpracováním osobních údajů*, bod 1 přehledu podkladů, str. 3-4). Zaměstnanec kontrolované osoby má pak možnost evidovat svoji docházku jak pomocí [REDAKCE] čipu (který rovněž slouží k otevírání vstupních dveří), tak přiložením prstu k docházkovému terminálu. Kontrolovaná osoba vnímá využití otisků prstů jako záložní metodu, neboť se dle jejího vyjádření stává, že zaměstnanci zapomínají čipy přinést s sebou na pracoviště a také je mechanicky poškozují (bod 4 přehledu podkladů, str. 2).

Kontrolující uvádějí, že byť kontrolovaná osoba opírá zpracování biometrických údajů v podobě hashů otisků prstů zaměstnanců kontrolované osoby o jejich souhlas, tak získání souhlasu neruší ani nijak nesnižuje povinnosti kontrolované osoby jako správce dodržovat zásady zpracování zakotvené v nařízení (EU) 2016/679, zejména čl. 5 nařízení (EU) 2016/679, pokud jde o nezbytnost a přiměřenost údajů. I když je zpracování osobních údajů založeno na souhlasu subjektu údajů, neospravedlňuje shromažďování údajů, jež nejsou nezbytné ve vztahu ke stanovenému účelu zpracování¹. Jinými slovy i v případě, že je zpracování osobních údajů založeno na souhlasu s určitým zpracováním osobních údajů, tak platí, že je vždy možno zpracovávat osobní údaje pouze v tom rozsahu, který je nezbytný k naplnění sledovaného účelu. Tato zásada vyjádřená v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679, platí pro každé zpracování osobních údajů, lhostejno na jakém právním základě je položeno.

Shromažďování hashů otisků prstů zaměstnanců není ve vztahu ke stanovenému účelu nezbytné. Kontrolovaná osoba může využívat jiný způsob evidence docházky zaměstnanců, nezávislý na udělení jejich souhlasu a nevyužívající biometrické údaje jakožto zvláštní kategorii osobních údajů dle čl. 9 nařízení (EU) 2016, které jsou svou povahou obzvláště citlivé z hlediska základních práv a svobod, a při jejichž zpracování mohou vznikat závažná rizika pro základní práva a svobody.

Kontrolovaná osoba takový méně rizikový způsob současně využívá, a to v podobě  čipů. Tyto obdrží všichni zaměstnanci a všem je zaveden do docházkového systému, bez ohledu na to, zda udělili souhlas se zpracováním hashů otisků prstů, a slouží též k otevírání vstupních dveří do zaměstnání. Jak je zřejmé z vyjádření kontrolované osoby, hashe otisků prstů jsou alternativou proti využití čipu, kterou může zaměstnanec využít např. na základě své preference či opomenutí nebo poškození čipu.

Kontrolovaná osoba porušila čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679 (tj. zásadu minimalizace údajů), neboť v období od měsíce dubna roku 2022 do data vydání tohoto protokolu zpracovávala v elektronickém docházkovém systému hashe otisku prstů svých zaměstnanců, v celkovém souhrnném počtu nejméně 57 subjektů údajů, byť tyto údaje nebyly nezbytné ve vztahu k účelu evidence docházky zaměstnanců.

IV. Povinnost podat zprávu dle § 10 odst. 2 zákona č. 255/2012 Sb.

Kontrolující v souladu s ustanovením § 10 odst. 2 zákona č. 255/2012 Sb., o kontrole (kontrolní řád) (dále jen „zákon č. 255/2012 Sb.“) žádají kontrolovanou osobu o podání písemné zprávy o odstranění nedostatků zjištěných kontrolou, a to ve lhůtě 30 dnů ode dne formálního ukončení kontroly ve smyslu § 18 zákona č. 255/2012 Sb. Za splnění této povinnosti lze považovat i podání zprávy o opatřeních, která budou v danou dobu stále ve fázi přípravy nebo realizace.

Kontrolující v dané věci upozorňují na to, že v souladu s § 15 zákona č. 255/2012 Sb. je nesplnění povinnosti dle § 10 odst. 2 tohoto zákona považováno za přestupek, za který lze

¹ Pokyny č. 05/2020 k souhlasu podle nařízení 2016/679, Verze 1.1, Přijato dne 4. května 2020, str. 5-6, dostupné z: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_cs.pdf.

uložit pokutu do výše 500 000 Kč. V případě, že kontrolovaná osoba nebude z objektivních důvodů schopna podat písemnou zprávu o odstranění nebo prevenci nedostatků, zjištěných kontrolou ve stanoveném termínu, lze před vypršením stanovené lhůty písemně požádat kontrolní orgán o její prodloužení.

V. 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.

VI. Podpisová doložka:

Mgr. Marek Šnajdr	vedoucí kontrolní skupiny pověřený zaměstnanec Úřadu	<u>(podepsáno elektronicky)</u> podpis
Mgr. Jaromír Kuba	pověřený zaměstnanec Úřadu	<u>(podepsáno elektronicky)</u> podpis
Bc. Šárka Hozmanová	pověřená zaměstnankyně Úřadu	<u>(podepsáno elektronicky)</u> podpis