Usmernenia 3/2019 k spracúvaniu osobných údajov prostredníctvom kamerových zariadení

Verzia 2.0

Prijaté 29. januára 2020

História verzií

Verzia 2.0	29. januára 2020	Prijatie usmernení po verejnej konzultácii
Verzia 1.0	streda 10. júla 2019	Prijatie usmernení na účely verejnej konzultácie

Obsah

Európsky výbor pre ochranu údajov

so zreteľom na článok 70 ods. 1 písm. e) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“),

so zreteľom na Dohodu o EHP, a najmä na jej prílohu XI a protokol 37, v znení rozhodnutia Spoločného výboru EHP č. 154/2018 zo 6. júla 2018,[1]

so zreteľom na článok 12 a článok 22 svojho rokovacieho poriadku,

PRIJAL TIETO USMERNENIA

1 ÚVOD

1. Intenzívne používanie kamerových zariadení ovplyvňuje správanie občanov. Keďže sa tieto nástroje používajú v mnohých oblastiach života a vo veľkej miere, zvyšuje sa tlak na jednotlivcov, aby sa usilovali zabrániť odhaleniu niečoho, čo sa môže vnímať ako anomália. V skutočnosti môžu tieto technológie obmedzovať možnosti anonymného pohybu alebo anonymného využívania služieb a vo všeobecnosti obmedzovať možnosť zostať nepovšimnutý. Dopady na ochranu údajov sú obrovské.

2. Aj keď jednotlivci nemusia mať výhrady voči monitorovaniu kamerou zriadenou napríklad na určitý bezpečnostný účel, treba prijať záruky, aby sa predišlo akémukoľvek zneužitiu na úplne odlišné a – pre dotknutú osobu – neočakávané účely (napr. marketingový účel, monitorovanie výkonnosti zamestnancov atď.). Okrem toho sa používa množstvo nástrojov, ktorými možno využiť zachytené snímky a premeniť obyčajné kamery na smart kamery. Množstvo údajov, ktoré pochádza z videozáznamov, v kombinácii s takýmito nástrojmi a technikami zvyšuje riziká sekundárneho použitia (či už v súvislosti s pôvodným účelom systému, alebo nie), či dokonca riziká ich zneužitia. Pri monitorovaní kamerou treba vždy starostlivo zvážiť všeobecné zásady stanovené vo všeobecnom nariadení o ochrane údajov (článok 5).

3. Monitorovanie kamerovými systémami z rôznych hľadísk mení spôsob, akým odborníci zo súkromného a z verejného sektora spolupracujú na súkromných alebo verejných miestach, a to na účely zvýšenia bezpečnosti, získavania analýzy publika, poskytovania personalizovanej reklamy atď. Vďaka čoraz rozšírenejšiemu používaniu inteligentných analýz videí sa z monitorovania kamerou stal vysokovýkonný proces. Tieto techniky môžu byť rušivejšie (napr. zložité biometrické technológie) alebo menej rušivé (napr. jednoduché výpočtové algoritmy). Zachovanie anonymity a ochrana vlastného súkromia sú vo všeobecnosti čoraz zložitejšie. Otázky spojené s ochranou osobných údajov sa môžu v jednotlivých situáciách líšiť, podobne ako ich právna analýza, pri použití niektorej z týchto technológií.

[1] Odkazy na „členské štáty“ uvedené v tomto stanovisku by sa mali chápať ako odkazy na „členské štáty EHP“.

4. Okrem otázok spojených s ochranou súkromia, existujú aj riziká súvisiace s možným nesprávnym fungovaním týchto zariadení a neobjektívnosťou, ku ktorej môžu viesť. Výskumní pracovníci uvádzajú, že softvér používaný na identifikáciu, rozpoznávanie alebo analýzu tvárí sa správa inak v závislosti od veku, pohlavia a etnického pôvodu osoby, ktorú identifikuje. Algoritmy by teda poskytovali výsledky na základe rôznych demografických faktorov, a preto hrozí, že neobjektívnosť v rozpoznávaní tvárí môže posilňovať predsudky spoločnosti. Z tohto dôvodu musia prevádzkovatelia zabezpečiť, aby spracúvanie biometrických údajov pochádzajúcich z monitorovania kamerou bolo predmetom pravidelného hodnotenia z hľadiska relevantnosti a dostatočnosti poskytnutých záruk.

5. Monitorovanie kamerou nie je štandardne nevyhnutnosťou, ak existujú iné prostriedky na dosiahnutie požadovaného účelu. V opačnom prípade riskujeme zmenu v kultúrnych normách, ktorá povedie k akceptovaniu nedostatku súkromia ako všeobecného nastavenia.

6. V týchto usmerneniach sa poskytujú rady, ako uplatňovať všeobecné nariadenie o ochrane údajov v súvislosti so spracúvaním osobných údajov prostredníctvom kamerových zariadení. Tieto príklady nie sú vyčerpávajúce, avšak všeobecné zdôvodnenie je možné uplatniť vo všetkých potenciálnych oblastiach použitia.

2 ROZSAH PÔSOBNOSTI[2]

2.1 Osobné údaje

7. V súčasnosti sa systematické automatické monitorovanie konkrétneho priestoru optickými alebo audiovizuálnymi prostriedkami, predovšetkým na účely ochrany majetku alebo na ochranu života a zdravia jednotlivca, stalo výrazným javom. Táto činnosť je spojená so získavaním a s uchovávaním obrazových alebo audiovizuálnych informácií o všetkých osobách vstupujúcich do monitorovaného priestoru, ktoré sú identifikovateľné na základe vzhľadu a iných osobitných čŕt. Identifikácia týchto osôb môže byť založená na základe týchto údajov. Takisto to umožňuje ďalej spracúvať osobné údaje, pokiaľ ide o prítomnosť osoby a jej správanie na danom mieste. Potenciálne riziko zneužitia týchto údajov rastie s rozmermi monitorovaného priestoru, ako aj s počtom osôb, ktoré toto miesto pravidelne navštevujú. Táto skutočnosť sa odráža vo všeobecnom nariadení o ochrane údajov v článku 35 ods. 3 písm. c), ktorý vyžaduje, aby sa vykonalo posúdenie vplyvu na ochranu údajov v prípade systematického monitorovania verejne prístupných miest vo veľkom rozsahu, ako aj v článku 37 ods. 1 písm. b), ktorý vyžaduje, aby sprostredkovatelia určili zodpovednú osobu, ak spracovateľská operácia vzhľadom na svoju povahu zahŕňa pravidelné a systematické monitorovanie dotknutých osôb.

8. Avšak, ak na základe spracúvaných údajov, napríklad nie je možné konkrétnu osobu priamo alebo nepriamo identifikovať, všeobecné nariadenia o ochrane údajov sa na takéto spracúvanie nevzťahuje

> Príklad: Všeobecné nariadenie o ochrane údajov sa neuplatňuje na falošné kamery (t. j. akákoľvek kamera, ktorá nefunguje ako kamera, a preto nespracúva osobné údaje). *V niektorých členských štátoch však tento prípad môže podliehať iným právnym predpisom.*
>
> Príklad: Záznamy z veľkej výšky patria do rozsahu pôsobnosti všeobecného nariadenia o ochrane údajov, pokiaľ v danej situácii spracúvané údaje možno spojiť s konkrétnou osobou.
>
> Príklad: Kamera je súčasťou výbavy auta ako pomoc pri parkovaní. Ak je kamera zostrojená alebo prispôsobená tak, že nezískava žiadne informácie týkajúce sa fyzickej osoby (ako sú tabuľky s evidenčným číslom vozidla alebo informácie, na základe ktorých by bolo možné identifikovať okoloidúcich), všeobecné nariadenie o ochrane údajov sa neuplatňuje.

9.

2.2 Uplatňovanie smernice (EÚ) 2016/680 o presadzovaní práva

10. Do rozsahu pôsobnosti smernice (EÚ) 2016/680 patrí predovšetkým spracúvanie osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií, vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu.

2.3 Výnimka pre domáce činnosti

11. Podľa článku 2 ods. 2 písm. c) do rozsahu pôsobnosti všeobecného nariadenia o ochrane údajov nepatrí spracúvanie osobných údajov vykonávané fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti, čo môže takisto zahŕňať online činnosť.[3]

[2] EDPB upozorňuje, že ak to všeobecné nariadenie o ochrane údajov umožňuje, môžu sa uplatňovať osobitné požiadavky stanovené vo vnútroštátnych právnych predpisoch.

[3] Pozri aj odôvodnenie 18.

12. Toto ustanovenie – nazývané aj výnimka pre domáce činnosti – sa musí v kontexte monitorovania kamerou vykladať úzko. V dôsledku toho a v súlade so záverom Európskeho súdneho dvora sa takzvaná „výnimka pre domáce činnosti“ musí „*vykladať tak, že sa vzťahuje výlučne na činnosti, ktoré patria do rámca súkromného alebo rodinného života jednotlivcov, čo zjavne neplatí v prípade spracúvania osobných údajov, ktoré spočíva v ich zverejnení na internete takým spôsobom, že sa sprístupnia neobmedzenému počtu osôb.*“[4] Okrem toho, pokiaľ monitorovanie kamerovým systémom zahŕňa nepretržité zaznamenávanie a uchovávanie osobných údajov a pokrýva „*hoci len čiastočne, verejné priestranstvo, a smeruje mimo súkromnú sféru osoby, ktorá jeho prostredníctvom spracúva údaje, nemožno ho považovať za výlučne ‘osobnú či domácu‘ činnosť v zmysle článku 3 ods. 2 druhej zarážky smernice 95/46.*“[5].

13. Pokiaľ ide o používanie kamerových zariadení v priestoroch súkromnej osoby, výnimka pre domáce činnosti sa naň môže vzťahovať. Takýto záver bude závisieť od niekoľkých faktorov, ktoré je potrebné všetky zvážiť. Okrem uvedených prvkov identifikovaných v rozhodnutiach SDEÚ musí osoba uskutočňujúca monitorovanie kamerou u seba doma zohľadniť, či má s dotknutou osobou nejaký druh osobného vzťahu, či rozsah alebo frekvencia monitorovania nenasvedčuje, že ide z jeho strany o profesionálnu činnosť, a takisto musí zohľadniť možný negatívny účinok monitorovania na dotknuté osoby. Prítomnosť ktoréhokoľvek z uvedených prvkov nemusí nevyhnutne znamenať, že ide o spracúvanie mimo rozsahu výnimky pre domáce činnosti, pričom na takéto určenie sa vyžaduje celkové posúdenie.

> Príklad: Turista nahráva videá na zdokumentovanie svojej dovolenky pomocou mobilného telefónu a digitálnej kamery. Záznam ukáže priateľom a rodine, ale nesprístupní ho neobmedzenému množstvu ľudí. Na toto by sa vzťahovala výnimka pre domáce činnosti.
>
> Príklad: Horská cyklistka si chce pomocou akčnej kamery zaznamenať svoj zjazd. Bicykluje sa vo vzdialenej oblasti a svoje záznamy plánuje použiť len na vlastnú zábavu doma. Na toto by sa vzťahovala výnimka pre domáce činnosti, hoci sa osobné údaje do určitej miery spracúvajú.
>
> Príklad: Niekto monitoruje a robí záznam vlastnej záhrady. Pozemok je ohradený a do záhrady pravidelne vstupuje len samotný prevádzkovateľ a jeho rodina. Na toto by sa vzťahovala výnimka pre domáce činnosti, pokiaľ monitorovanie kamerou nepokrýva hoci len čiastočne aj verejný priestor alebo susedný pozemok.

14.

[4] Európsky Súdny dvor, rozsudok zo 6. novembra 2003 vo veci C-101/01, Bodil Lindqvist, bod 47.

[5] Európsky súdny dvor, rozsudok z 11. decembra 2014 vo veci C-212/13, František Ryneš/Úřad pro ochranu osobních údajů, bod 33.

3 ZÁKONNOSŤ SPRACÚVANIA

15. Pred použitím sa musia podrobne uviesť účely spracúvania [článok 5 ods. 1 písm. b)]. Monitorovanie kamerou môže slúžiť na mnohé účely, napr. na zlepšenie ochrany nehnuteľnosti a iného majetku, na zvýšenie ochrany života a telesnej integrity jednotlivcov, získanie dôkazov na účely občianskoprávnych nárokov.[6] Tieto účely monitorovania treba písomne zdokumentovať (článok 5 ods. 2) a musia byť uvedené pre každú používanú monitorovaciu kameru. V prípade kamier, ktoré používa jeden prevádzkovateľ na rovnaký účel, možno vyhotoviť spoločnú dokumentáciu. Okrem toho dotknuté osoby musia byť informované o účele(-och) spracúvania v súlade s článkom 13 (*pozri oddiel 7, Požiadavky na transparentnosť a informačnú povinnosť*). Monitorovanie kamerou označené iba ako účel „bezpečnosti“ alebo „vlastnej bezpečnosti“ nie je dostatočne konkrétny [článok 5 ods. 1 písm. b)]. Navyše je to v rozpore so zásadou, podľa ktorej osobné údaje musia byť spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe [článok 5 ods. 1 písm. a)].

16. Právny základ na spracúvanie údajov získaných prostredníctvom monitorovania kamerou môže v zásade predstavovať každý právny základ podľa článku 6 ods. 1. Napríklad v prípade, že vo vnútroštátnom práve je stanovená povinnosť vykonávať monitorovanie kamerou, uplatňuje sa článok 6 ods. 1 písm. c).[7] Avšak, v praxi sa s najväčšou pravdepodobnosťou použijú ustanovenia:

- článku 6 ods. 1 písm. f) (oprávnený záujem),
- článku 6 ods. 1 písm. e) (nevyhnutnosť na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci).

Vo výnimočných prípadoch môže prevádzkovateľ použiť ako právny základ článok 6 ods. 1 písm. a) (súhlas).

3.1 Oprávnený záujem, článok 6 ods. 1 písm. f)

17. Právne posúdenie článku 6 ods. 1 písm. f) by sa malo zakladať na nasledujúcich kritériách v súlade s odôvodnením 47.

3.1.1 Existencia oprávnených záujmov

18. Monitorovanie kamerou je v súlade s právom, ak je nevyhnutné na účel oprávneného záujmu, ktorý sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby [článok 6 ods. 1 písm. f)]. Oprávnené záujmy sledované prevádzkovateľom alebo treťou stranou môžu byť právne[8], hospodárske alebo nemajetkové záujmy.[9] Prevádzkovateľ by však mal vziať do úvahy, že ak dotknutá osoba namieta voči monitorovaniu v súlade s článkom 21, prevádzkovateľ môže pristúpiť k monitorovaniu tejto dotknutej osoby kamerovým systémom iba vtedy, keď ide o *závažný* [compelling] oprávnený záujem, ktorý prevažuje nad záujmami, právami a slobodami dotknutej osoby, alebo ide o dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

---

[6] Pravidlá týkajúce sa získavania dôkazov na účely občianskoprávnych nárokov sa v členských štátoch rôznia.

[7] V týchto usmerneniach sa neanalyzuje ani podrobne nerozoberá vnútroštátne právo, ktoré sa môže medzi jednotlivými členským štátmi líšiť.

[8] Európsky súdny dvor, rozsudok zo 4. mája 2017 vo veci C-13/16, Rīgas satiksme.

[9] Pozri WP 217, pracovná skupina zriadená podľa článku 29.

19. V prípade skutočnej a nebezpečnej situácie môže účel ochrany majetku proti vlámaniu, krádeži alebo vandalizmu predstavovať oprávnený záujem pre monitorovanie kamerou.

20. Oprávnený záujem musí skutočne existovať a byť aktuálny (t. j. nemôže byť fiktívny ani špekulatívny)[10]. Mal by vychádzať zo skutočnej tiesňovej situácie – ako sú škody alebo vážne incidenty v minulosti – ku ktorým došlo pred začiatkom monitorovania. Na základe zásady zodpovednosti sa prevádzkovateľom odporúča, aby zdokumentovali príslušné incidenty (dátum, spôsob, finančnú stratu) a súvisiace trestné obvinenia. Takéto zdokumentované incidenty môžu predstavovať presvedčivý dôkaz existencie oprávneného záujmu. Existenciu oprávneného záujmu, ako aj nevyhnutnosť monitorovania je potrebné v pravidelných intervaloch prehodnocovať (napr. raz za rok, v závislosti od okolností).

> Príklad: Majiteľ predajne chce otvoriť novú prevádzku a nainštalovať systém na monitorovanie kamerou na účely predchádzania vandalizmu. Prostredníctvom štatistiky môže preukázať, že v blízkom okolí je vysoký predpoklad vandalizmu. Skúsenosti susedných prevádzok sú takisto užitočné. Nevyžaduje sa, aby dotknutý prevádzkovať preukázal vzniknutú škodu. Pokiaľ škody v susedstve naznačujú nebezpečenstvo a pod., môže to preukazovať oprávnený záujem. Predloženie národných alebo všeobecných štatistík trestných činov, bez analýzy dotknutej oblasti alebo nebezpečenstiev pre túto konkrétnu predajňu, však nie je dostatočné.

21.

22. Oprávnený záujem môžu predstavovať situácie bezprostredného nebezpečenstva. Ide napríklad o banky alebo obchody predávajúce vzácny tovar (napr. klenotníctva) či oblasti známe ako typické miesta majetkových trestných činov (napr. čerpacie stanice).

23. Vo všeobecnom nariadení o ochrane údajov sa jasne stanovuje, že verejné orgány nemôžu svoje spracúvanie zdôvodňovať oprávneným záujmom, ak ide o výkon ich úloh (článok 6 ods. 1 druhá veta).

3.1.2 Nevyhnutnosť spracúvania

24. Osobné údaje by mali byť primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú („minimalizácia údajov“), pozri článok 5 ods. 1 písm. c). Pred nainštalovaním systému na monitorovanie kamerou by mal prevádzkovateľ vždy kriticky preskúmať, či je toto opatrenie v prvom rade vhodné na dosiahnutie želaného cieľa a v druhom rade primerané a nevyhnutné na dané účely. Opatrenia spočívajúce v monitorovaní kamerou by sa mali zvoliť len vtedy, keď účel spracúvania nemožno primerane dosiahnuť inými prostriedkami, ktoré v menšej miere narúšajú základné práva a slobody dotknutej osoby.

25. V prípade situácie, ak chce prevádzkovateľ zamedziť majetkovým trestným činom, mohol by namiesto inštalácie systému na monitorovanie kamerou prijať náhradné bezpečnostné opatrenia, ako je oplotenie majetku, zavedenie pravidelných pochôdzok bezpečnostného personálu, využívanie vrátnikov, zabezpečenie lepšieho osvetlenia, inštalácia bezpečnostných zámkov, bezpečnostných okien a dverí alebo nanesenie náterov či fólií na múry na ochranu proti grafitom. Takéto opatrenia môžu byť rovnako účinné proti vlámaniam, krádežiam a vandalizmu ako systém na monitorovanie kamerou. Prevádzkovateľ musí v jednotlivých prípadoch posúdiť, či môžu byť takéto opatrenia vhodným riešením.

26. Pred uvedením kamerového systému do prevádzky musí prevádzkovateľ posúdiť, kde a kedy sú opatrenia na monitorovanie kamerou prísne nevyhnutné. Zvyčajne bude na naplnenie potrieb

[10] Pozri WP 217, pracovná skupina zriadená podľa článku 29, s. 24 a nasl. Pozri aj SDEÚ, C-708/18, bod 44.

prevádzkovateľa v súvislosti s predchádzaním ohrozeniu jeho majetku stačiť monitorovanie kamerovým systémom v noci a mimo pravidelných prevádzkových hodín.

27. Vo všeobecnosti je potreba používania monitorovania kamerou na ochranu prevádzkovateľových priestorov obmedzená hranicami majetku.[11] Existujú však prípady, keď monitorovanie majetku nie je na účinnú ochranu dostatočné. V niektorých prípadoch môže byť potrebné rozšíriť monitorovanie kamerou na bezprostredné okolie priestorov. V tomto kontexte by prevádzkovateľ mal zvážiť fyzické a technické prostriedky, ako je blokovanie alebo pixelovanie oblastí, ktoré nie sú relevantné.

> Príklad: Kníhkupectvo chce chrániť svoje priestory pred vandalizmom. Vo všeobecnosti by kamery mali zaznamenávať iba samotné priestory, pretože na tento účel nie je potrebné sledovať susediace priestory ani verejné priestory v okolí kníhkupectva.

28.

29. Otázky týkajúce sa nevyhnutnosti spracúvania vyvstávajú aj v súvislosti so spôsobom uchovávania dôkazov. V niektorých prípadoch môže byť potrebné použiť riešenia čiernej skrinky, keď sa záznam automaticky odstráni po určitej dobe uchovávania a sprístupní sa len v prípade incidentu. V iných situáciách nemusí byť potrebné videozáznamy vôbec nahrávať, ale vhodnejšie je namiesto toho použiť monitorovanie v reálnom čase. Rozhodnutie medzi riešeniami čiernej skrinky a monitorovaním v reálnom čase by malo vychádzať aj zo sledovaného účelu. Ak je napríklad účelom monitorovania kamerou uchovávanie dôkazov, metódy v reálnom čase zvyčajne nie sú vhodné. Monitorovanie v reálnom čase môže byť niekedy rušivejšie ako ukladanie a automatické odstraňovanie materiálu po uplynutí stanovenej lehoty (napr. môže byť rušivejšie, ak niekto nepretržite sleduje monitor ako v prípade, že sa monitor vôbec nepoužíva a materiál je priamo uložený v čiernej skrinke). V tomto kontexte treba zohľadňovať zásadu minimalizácie údajov [článok 5 ods. 1 písm. c)]. Rovnako treba mať na pamäti, že prevádzkovateľ by prípadne mohol namiesto monitorovania kamerou využívať bezpečnostných zamestnancov, ktorí môžu okamžite reagovať a zasiahnuť.

3.1.3 Porovnávanie záujmov

30. Za predpokladu, že monitorovanie kamerou je nevyhnutné na ochranu oprávnených záujmov prevádzkovateľa, systém na monitorovanie kamerou možno uviesť do prevádzky, len ak nad oprávnenými záujmami prevádzkovateľa alebo záujmami tretej strany (napr. ochrana majetku alebo telesnej integrity) neprevažujú záujmy alebo základné práva a slobody dotknutej osoby. Prevádzkovateľ musí zohľadniť: 1. do akej miery monitorovanie ovplyvňuje záujmy, základné práva a slobody jednotlivcov a 2. či tým spôsobuje porušovanie práv dotknutej osoby alebo negatívne dôsledky na tieto práva. Treba zdôrazniť, že porovnávanie záujmov je povinné. Základné práva a slobody na jednej strane a oprávnené záujmy prevádzkovateľa na druhej strane musia byť dôkladne preskúmané a porovnané.

[11] Toto môže v niektorých členských štátoch podliehať vnútroštátnym právnym predpisom.

Príklad: Súkromná parkovacia spoločnosť zaznamenáva opakujúce sa problémy vykrádania zaparkovaných áut. Parkovisko je otvorené a je ľahko dostupné pre všetkých, ale je jasne označené značkami a cestnými zábranami, ktoré priestor ohraničujú. Parkovacia spoločnosť má oprávnený záujem (predchádzať vykrádaniu áut zákazníkov) na monitorovaní priestoru v čase, keď dochádza k problémom. Dotknuté osoby sú monitorované v obmedzenom časovom rozsahu, nenachádzajú sa v priestore na rekreačné účely a predchádzanie vykrádaniu je takisto v ich záujme. V tomto prípade oprávnený záujem prevádzkovateľa prevažuje nad záujmom dotknutých osôb na tom, aby neboli monitorované.

Príklad: Reštaurácia sa rozhodne nainštalovať videokamery na toaletách, aby kontrolovala čistotu hygienických zariadení. V tomto prípade práva dotknutých osôb jasne prevažujú nad záujmami prevádzkovateľa, preto tu kamery nemožno nainštalovať.

31.

3.1.3.1 Rozhodovanie sa na základe jednotlivých prípadov

32. Keďže podľa nariadenia je porovnávanie záujmov povinné, rozhodnutie sa musí prijať na základe jednotlivých prípadov [článok 6 ods. 1. písm. f)]. Odkazovanie na abstraktné situácie alebo vzájomné porovnávanie podobných prípadov nie je dostatočné. Prevádzkovateľ musí posúdiť riziká narušenia práv dotknutej osoby; v tomto prípade je rozhodujúcim kritériom závažnosť zásahu do práv a slobôd jednotlivca.

33. Závažnosť možno okrem iného vymedziť na základe informácií, ktoré sa získavajú (obsah informácií), rozsahu (hustota informácií, priestorový a geografický rozsah), počtu dotknutých osôb, a to buď ako konkrétne číslo, alebo ako podiel príslušnej populácie, príslušnej situácie, skutočných záujmov skupiny dotknutých osôb, alternatívnych prostriedkov, ako aj povahy a rozsahu posudzovania údajov.

34. Významnými porovnávacími faktormi [balancing factors] môžu byť veľkosť oblasti, ktorá sa monitoruje, a počet dotknutých osôb, ktoré sú predmetom monitorovania. Používanie monitorovania kamerou vo vzdialenej oblasti (napr. na sledovanie voľne žijúcich druhov alebo na ochranu kritickej infraštruktúry, ako je rádiový vysielač v súkromnom vlastníctve) sa musí posudzovať inak ako monitorovanie kamerou na pešej zóne alebo v nákupnom centre.

Príklad: Ak je nainštalovaná autokamera (napr. na účely získania dôkazov v prípade nehody), treba zabezpečiť, aby táto kamera nezaznamenávala dopravu nepretržite, ako ani osoby, ktoré sa nachádzajú pri ceste. V opačnom prípade, záujem mať videozáznamy ako dôkaz v hypotetickom prípade dopravnej nehody, nie je možné odôvodňovať takýmto závažným zásahom do práv dotknutých osôb.[11]

35.

3.1.3.2 Primerané očakávania dotknutých osôb

36. V súlade s odôvodnením 47 si existencia oprávneného záujmu vyžaduje dôkladné posúdenie. Treba sem zahrnúť primerané očakávania dotknutej osoby v čase a kontexte spracúvania jej osobných údajov. Pokiaľ ide o systematické monitorovanie, vzťah medzi dotknutou osobou a prevádzkovateľom sa môže výrazne odlišovať a mať vplyv na primerané očakávania, ktoré dotknutá osoba môže mať. Výklad pojmu primerané očakávania by nemal vychádzať z príslušných subjektívnych očakávaní. Rozhodujúcim kritériom naopak musí byť, či objektívna tretia strana mohla primerane očakávať a dospieť k záveru, že bude v tejto konkrétnej situácii predmetom monitorovania.

37. Napríklad zamestnanec na svojom pracovisku vo väčšine prípadov neočakáva, že ho bude zamestnávateľ monitorovať.[12] Okrem toho sa monitorovanie neočakáva ani vo vlastnej súkromnej záhrade, obytnom priestore, ani v ordinácii či ošetrovni. Podobne nie je primerané očakávať monitorovanie v hygienických či saunových zariadeniach – monitorovanie v takýchto priestoroch je závažným narušením práv dotknutej osoby. Primerané očakávania dotknutých osôb spočívajú v tom, že sa v takýchto priestoroch nebude vykonávať žiadne monitorovanie kamerou. Na druhej strane zákazník banky môže očakávať, že v interiéri banky alebo pri bankomate bude monitorovaný.

38. Dotknuté osoby môžu takisto očakávať, že nebudú monitorované na verejne dostupných miestach, a to najmä ak sú tieto miesta zvyčajne využívané na zotavenie, regeneráciu a voľnočasové aktivity, ako aj na miestach, kde sa ľudia zdržiavajú a/alebo zhovárajú, ako sú zóny na sedenie, stoly v reštauráciách, parky, kiná a fitnes zariadenia. V tomto prípade záujmy či práva a slobody dotknutej osoby často prevážia nad oprávnenými záujmami prevádzkovateľa.

> Príklad: Dotknuté osoby očakávajú, že na toaletách nebudú monitorované. Monitorovanie kamerou, napr. na predchádzanie nehodám, v takomto prípade nie je primerané.

39.

40. Označenia informujúce dotknutú osobu o monitorovaní kamerou nemajú pri určovaní toho, čo dotknutá osoba môže objektívne očakávať význam. To znamená, že napr. majiteľ predajne sa nemôže spoliehať na to, že zákazníci majú *objektívne* primerané očakávania, že budú monitorovaní, len preto, že pri vchode je označenie informujúce osoby o monitorovaní.

3.2 Nevyhnutnosť z hľadiska splnenia úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi [článok 6 ods. 1 písm. e)]

41. Osobné údaje možno spracúvať prostredníctvom monitorovania kamerou podľa článku 6 ods. 1 písm. e), ak je to nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci.[13] Môže sa vyskytnúť situácia, keď výkon verejnej moci neumožňuje takéto spracúvanie, ale iné právne základy, ako je „zdravie a bezpečnosť“ na účely ochrany návštevníkov alebo zamestnancov, môžu poskytovať obmedzený rámec pre spracúvanie, pričom sa stále zohľadňujú povinnosti podľa všeobecného nariadenia o ochrane údajov a práva dotknutých osôb.

42. Členské štáty môžu zachovať alebo zaviesť osobitné vnútroštátnu právnu úpravu na monitorovanie kamerou s cieľom prispôsobiť uplatňovanie pravidiel všeobecného nariadenia o ochrane údajov presnejším určením osobitných požiadaviek na spracúvanie, pokiaľ je to v súlade so zásadami stanovenými vo všeobecnom nariadení o ochrane údajov (napr. obmedzenie ukladania, primeranosť).

[12] Pozri aj: Pracovná skupina zriadená podľa článku 29, Stanovisko 2/2017 k spracúvaniu údajov na pracovisku, WP 249, prijaté 8. júna 2017.

[13] Základ pre uvedené spracúvanie musí byť stanovený v práve Únie alebo práve členského štátu, pričom spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi (článok 6 ods. 3).

3.3 Súhlas, článok 6 ods. 1 písm. a)

43. Súhlas musí byť slobodne daný, konkrétny, informovaný a jednoznačný, ako sa opisuje v usmerneniach k súhlasu.[14]

44. Pokiaľ ide o systematické monitorovanie, súhlas dotknutej osoby môže slúžiť ako právny základ v súlade s článkom 7 (pozri odôvodnenie 43) len vo výnimočných prípadoch. Monitorovanie je charakteristické tým, že táto technológia monitoruje neznámy počet osôb súčasne. Prevádzkovateľ bude sotva môcť dokázať, že dotknutá osoba vyjadrila pred spracúvaním jej osobných údajov súhlas (článok 7 ods. 1). V prípade, že dotknutá osoba odvolá svoj súhlas, pre prevádzkovateľa bude ťažké dokázať, že sa príslušné osobné údaje už nespracúvajú (článok 7 ods. 3).

> Príklad: Atléti môžu požiadať o monitorovanie počas jednotlivých cvičení na účely analyzovania ich techniky a výkonu. Na druhej strane, ak sa športový klub rozhodne monitorovať celý tím s tým istým účelom, súhlas často nebude platný, pretože jednotliví športovci sa môžu cítiť pod tlakom, aby súhlas udelili a aby ich odmietnutie súhlasu nemalo nepriaznivý vplyv na ostatných členov tímu.

45.

46. Ak sa prevádzkovateľ chce opierať o súhlas, je jeho povinnosťou uistiť sa, že každá dotknutá osoba vstupujúca do priestorov, ktoré sa monitorujú kamerou, poskytla svoj súhlas. Tento súhlas musí spĺňať podmienky článku 7. Vstup do označených monitorovaných priestorov (napr. keď sú ľudia vyzvaní, aby pred vstupom do monitorovaných priestorov prešli osobitnou chodbou alebo bránou) nepredstavuje vyhlásenie, ani jasné súhlasné vyjadrenie vyžadované na súhlas, pokiaľ to nespĺňa kritériá článkov 4 a 7, ako je opísané v usmerneniach k súhlasu.[15]

47. Vzhľadom na nepomer moci medzi zamestnávateľmi a zamestnancami by sa vo väčšine prípadov zamestnávatelia nemali pri spracúvaní údajov opierať o súhlas, keďže pravdepodobne nebol poskytnutý slobodne. V tejto súvislosti by mali byť zohľadnené usmernenia k súhlasu.

48. Právne predpisy členských štátov alebo kolektívne dohody, vrátane pracovných zmlúv, môžu poskytovať osobitné pravidlá na spracúvanie osobných údajov zamestnancov v súvislosti so zamestnaním (pozri článok 88).

[14] Pracovná skupina zriadená podľa článku 29, „Usmernenia k súhlasu podľa nariadenia 2016/679“ (WP 259 rev. 01). – schválené EDPB.

[15] Pracovná skupina zriadená podľa článku 29, „Usmernenia k súhlasu podľa nariadenia 2016/679“ (WP 259) – schválené EDPB – ktoré by mali byť zohľadnené.

4 POSKYTOVANIE VIDEOZÁZNAMOV TRETÍM STRANÁM

49. Na poskytovanie videozáznamov tretím stranám sa v zásade uplatňujú všeobecné ustanovenia všeobecného nariadenia o ochrane údajov.

4.1 Všeobecne o poskytovaní videozáznamu tretím stranám

50. Poskytovanie je vymedzené v článku 4 bode 2 ako prenos (napr. individuálne oznámenie), šírenie (online zverejnenie) alebo poskytovanie iným spôsobom. Tretie strany sú vymedzené v článku 4 bode 10. V prípade, že sa videozáznamy poskytujú tretím krajinám alebo medzinárodným organizáciám, uplatňujú sa aj osobitné ustanovenia článku 44 a nasl.

51. Každé poskytnutie osobných údajov je osobitným druhom spracúvania osobných údajov, na ktorý musí mať prevádzkovateľ právny základ uvedený v článku 6.

> Príklad: Prevádzkovateľ, ktorý chce nahrať záznam na internet, potrebuje na takéto spracúvanie právny základ, napr. získať súhlas dotknutých osôb podľa článku 6 ods. 1 písm. a).

52.

53. Prenos videozáznamu tretím stranám na účely, ktoré sú iné ako tie, na ktoré boli údaje získané, je možný v súlade s pravidlami uvedenými v článku 6 ods. 4.

> Príklad: Na účely predchádzania škodám je (na parkovisku) nainštalované monitorovanie rampy kamerou. Po vzniku škody sa záznam prenesie právnikovi, aby sa prípadom zaoberal. V tomto prípade je účel zaznamenávania rovnaký ako účel prenosu.
>
> Príklad: Na účely predchádzania škodám je (na parkovisku) nainštalované monitorovanie rampy kamerou. Tento záznam sa zverejní na internete výlučne na účely pobavenia. V tomto prípade sa účel zmenil a nie je v súlade s pôvodným účelom. Okrem toho by bolo problematické určiť právny základ pre takéto spracúvanie (zverejnenie).

54.

55. Prijímateľ, ktorý je treťou stranou, bude musieť vykonať vlastnú právnu analýzu, predovšetkým určiť právny základ podľa článku 6 pre vlastné spracúvanie (napr. prijatie materiálu).

4.2 Poskytovanie videozáznamov orgánom presadzovania práva

56. Poskytovanie videozáznamov orgánom presadzovania práva je takisto samostatným postupom, ktorý si vyžaduje samostatné odôvodnenie prevádzkovateľa.

57. V súlade s článkom 6 ods. 1 písm. c) je spracúvanie zákonné, ak je potrebné na dodržanie zákonnej povinnosti prevádzkovateľa, ktorej podlieha. Hoci platné právo v oblasti činnosti polície je otázkou, ktorá patrí do výhradnej kontroly jednotlivých členských štátov, s najväčšou pravdepodobnosťou, v každom členskom štáte existujú všeobecné pravidlá, ktorými sa upravuje prenos dôkazov orgánom presadzovania práva. Spracúvanie prevádzkovateľom, ktorý údaje odovzdáva, je upravené všeobecným nariadením o ochrane údajov. Ak sa vo vnútroštátnych právnych predpisoch vyžaduje, aby prevádzkovateľ spolupracoval s orgánmi presadzovania práva (napr. v prípade vyšetrovania), právnym základom pre odovzdanie údajov je zákonná povinnosť stanovená v článku 6 ods. 1 písm. c).

58. Obmedzenie účelu stanovené v článku 6 ods. 4 potom často nepredstavuje problém, keďže poskytnutie výslovne vychádza z právnych predpisov členského štátu. Zohľadnenie osobitných požiadaviek na zmenu účelu v zmysle písmen a) – e) preto nie je potrebné.

Príklad: Majiteľ predajne vyhotovuje kamerový záznam pri vchode. Na záznamoch je zachytený človek, ktorý kradne peňaženku druhému človeku. Polícia požiada prevádzkovateľa o odovzdanie materiálu na účely vyšetrovania. V takom prípade by majiteľ predajne mohol na účely spracúvania prenesených údajov použiť právny základ podľa článku 6 ods. 1 písm. c) (právna povinnosť) vykladaný v spojení s príslušnými vnútroštátnymi právnymi predpismi.

59.

Príklad: V predajni je z bezpečnostných dôvodov nainštalovaná kamera. Majiteľ obchodu je presvedčený, že na zázname je nahrané niečo podozrivé a rozhodne sa poslať materiál polícii (pričom neexistuje spojitosť so žiadnym prebiehajúcim vyšetrovaním). V tomto prípade musí majiteľ predajne posúdiť, či sú vo väčšine prípadov splnené podmienky stanovené v článku 6 ods. 1 písm. f). Ide zvyčajne o prípad, keď má majiteľ predajne odôvodnené podozrenie, že bol spáchaný trestný čin.

60.

61. Spracúvanie osobných údajov samotnými orgánmi presadzovania práva sa neriadi všeobecným nariadením o ochrane údajov [pozri článok 2 ods. 2 písm. d)], ale smernicou (EÚ) 2016/680 o presadzovaní práva.

5 SPRACÚVANIE OSOBITNÝCH KATEGÓRIÍ ÚDAJOV

62. Systémom na monitorovanie kamerou sa zvyčajne získavajú obrovské množstvá osobných údajov, ktoré môžu odhaliť údaje veľmi osobného charakteru a dokonca aj osobitnú kategóriu údajov. Zo zjavne nevýznamných údajov, ktoré sa pôvodne získali prostredníctvom videozáznamu, v skutočnosti možno odvodiť ďalšie informácie na dosiahnutie odlišného účelu (napr. na zmapovanie zvykov jednotlivca). Monitorovanie kamerou však nie je vždy považované za spracúvanie osobitných kategórií osobných údajov.

> Príklad: Videozáznam zobrazujúci dotknutú osobu s okuliarmi alebo na vozíku sa ako taký nepovažuje za záznam obsahujúci osobitné kategórie osobných údajov.

63.

64. Ak sa však tento videozáznam spracúva na odvodenie osobitných kategórií údajov, uplatňuje sa článok 9.

> Príklad: Zo zaznamenaných snímok identifikovateľných dotknutých osôb zúčastňujúcich sa na podujatí, zapájajúcich sa do štrajku a pod. by sa napríklad mohli odvodiť politické názory. Na tento prípad by sa vzťahoval článok 9.
>
> Príklad: Ak by nemocnica nainštalovala videokameru na monitorovanie pacientovho zdravotného stavu, považovalo by sa to za spracúvanie osobitných kategórií osobných údajov (článok 9).

65.

66. Vo všeobecnosti platí, že pri každej inštalácii systému na monitorovanie kamerou by sa mala dôsledne zohľadniť zásada minimalizácie údajov. Prevádzkovateľ by sa mal preto pokúsiť dokonca aj v prípadoch, keď sa neuplatňuje článok 9 ods. 1, minimalizovať záznam odhaľujúci iné citlivé údaje (nad rámec článku 9), a to bez ohľadu na cieľ.

> Príklad: Monitorovanie kamerou zachytávajúcou kostol nepatrí ako také do pôsobnosti článku 9. Prevádzkovateľ však pri posudzovaní záujmov dotknutej osoby musí vykonať osobitne dôkladné posúdenie podľa článku 6 ods. 1 písm. f) pri zohľadnení povahy údajov, ako aj rizika zachytenia citlivých údajov (nad rámec článku 9).

67.

68. Ak sa na spracúvanie osobitných kategórií údajov používa systém na monitorovanie kamerou, prevádzkovateľ musí určiť tak výnimku pre spracúvanie osobitných kategórií údajov podľa článku 9 (t. j. výnimku zo všeobecného pravidla, že osobitné kategórie údajov by sa nemali spracúvať), ako aj právny základ podľa článku 6.

69. Napríklad článok 9 ods. 2 písm. c) („[…] *spracúvanie je nevyhnutné na ochranu životne dôležitých záujmov dotknutej osoby* […]“) by sa – teoreticky a vo výnimočných prípadoch – mohol použiť, ale prevádzkovateľ by to musel odôvodniť ako absolútnu nevyhnutnosť na zabezpečenie životne dôležitých záujmov osoby a dokázať, že táto „[…] dotknutá osoba nie je *fyzicky alebo právne spôsobilá vyjadriť svoj súhlas*“. Okrem toho prevádzkovateľ nebude môcť použiť systém pre žiadny iný dôvod.

70. Treba tu poznamenať, že na odôvodnenie spracúvania osobitných kategórií údajov prostredníctvom monitorovania kamerou nebude pravdepodobne možné použiť každú výnimku uvedenú v článku 9. Presnejšie prevádzkovatelia spracúvajúci uvedené údaje v súvislosti s monitorovaním kamerou sa nemôžu opierať o článok 9 ods. 2 písm. e), ktorý umožňuje spracúvanie v súvislosti s osobnými údajmi

preukázateľne zverejnenými dotknutou osobou. Samotný vstup do záberu kamery neznamená, že dotknutá osoba plánuje zverejniť osobitné kategórie údajov, ktoré sa jej týkajú.

71. Okrem toho spracúvanie osobitných kategórií údajov si vyžaduje zvýšenú a neustálu obozretnosť, pokiaľ ide o určité povinnosti, ako je vysoká úroveň bezpečnosti a v prípade potreby posúdenie vplyvu na ochranu osobných údajov.

> Príklad: Zamestnávateľ nesmie použiť záznamy z monitorovania kamerou zobrazujúce demonštráciu na identifikáciu štrajkujúcich.

72.

5.1 Všeobecné otázky pri spracúvaní biometrických údajov

73. Používanie biometrických údajov a osobitne rozpoznávanie tvárí predstavuje zvýšené riziká pre práva dotknutých osôb. Je veľmi dôležité, aby sa pri používaní takýchto technológií dôsledne dodržiavali zásady zákonnosti, nevyhnutnosti, primeranosti a minimalizácie údajov, ako je stanovené vo všeobecnom nariadení o ochrane údajov. Zatiaľ čo používanie týchto technológií možno vnímať ako obzvlášť účinné, prevádzkovatelia by mali najprv posúdiť vplyv na základné práva a slobody a zvážiť menej rušivé prostriedky na dosiahnutie svojho oprávneného účelu spracúvania.

74. Spracúvanie surových údajov [raw data], ako sú fyzické, fyziologické alebo behaviorálne charakteristické znaky fyzickej osoby, možno kvalifikovať ako spracúvanie biometrických údajov podľa vymedzenia vo všeobecnom nariadení o ochrane údajov vtedy, keď zahŕňa meranie týchto charakteristík. Keďže biometrické údaje sú výsledkom takýchto meraní, v článku 4 bode 14 všeobecného nariadenia o ochrane údajov sa uvádza, že sú *„[…] výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby […]”.* Kamerové záznamy jednotlivca však ako také nemožno považovať za biometrické údaje v zmysle článku 9, ak neboli osobitne technicky spracúvané s cieľom prispieť k identifikácii jednotlivca.[16]

75. Na to aby mohlo ísť o spracúvanie osobitných kategórií osobných údajov (článok 9), musí byť splnená podmienka, že biometrické údaje sa spracúvajú „na jedinečnú identifikáciu fyzickej osoby“.

76. Možno zhrnúť, že vzhľadom na článok 4 bod 14 a článok 9 sa musia zohľadniť tri kritériá:

- **povaha údajov:** údaje týkajúce sa fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby,
- **prostriedky a spôsob spracúvania:** údaje, ktoré sú „výsledkom osobitného technického spracúvania“,
- **účel spracúvania:** údaje musia byť použité na účel jedinečnej identifikácie fyzickej osoby.

77. Používanie monitorovania kamerou, vrátane nainštalovanej funkcie rozpoznávania na základe biometrických údajov súkromnými subjektmi na vlastné účely (napr. marketingové, štatistické či

[16] V odôvodnení 51 všeobecného nariadenia o ochrane údajov sa takýto výklad podporuje, pričom sa v ňom uvádza, že *„[…] [s]pracúvanie fotografií by sa nemalo systematicky považovať za spracúvanie osobitných kategórií osobných údajov, pretože vymedzenie pojmu biometrické údaje sa na ne bude vzťahovať len v prípadoch, keď sa spracúvajú osobitnými technickými prostriedkami, ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu fyzickej osoby. […]*“.

bezpečnostné), si vo väčšine prípadov bude vyžadovať výslovný súhlas všetkých dotknutých osôb [článok 9 ods. 2 písm. a)], avšak mohla by sa použiť aj iná vhodná výnimka stanovená v článku 9.

Príklad: S cieľom zlepšiť svoje služby nahradí súkromná spoločnosť miesta kontroly identity cestujúcich na letisku (miesto na odovzdanie batožiny, odletová brána) systémom na monitorovanie kamerou na overenie totožnosti cestujúcich, ktorí vyjadrili súhlas s takýmto postupom, využíva techniky rozpoznávania tvárí. Keďže na takéto spracúvanie sa vzťahuje článok 9, cestujúci, ktorí vopred poskytli jasný a informovaný súhlas, sa budú musieť zaregistrovať napríklad na automatickom termináli, aby sa vytvoril a zaevidoval ich vzor tváre spojený s palubným lístkom a identitou. Kontrolné miesta so systémom na rozpoznávanie tvárí musia byť jasne oddelené, napr. systém musí byť nainštalovaný ako súčasť brány, aby sa nezachytávali biometrické vzory osôb, ktoré súhlas nevyjadrili. Bránu vybavenú systémom na zachytávanie biometrických údajov použijú len cestujúci, ktorí vopred poskytli súhlas a zaregistrovali sa.

Príklad: Prevádzkovateľ riadi prístup do svojej budovy prostredníctvom metódy rozpoznávania tvárí. Takýto spôsob prístupu môžu ľudia používať, len ak vopred poskytli výslovný informovaný súhlas [v súlade s článkom 9 ods. 2 písm. a)]. Aby sa zabezpečilo, že nebude zachytený nikto, kto predtým neposkytol súhlas, metódu rozpoznávania tvárí musí dotknutá osoba aktivovať sama, napríklad stlačením tlačidla. Na zaistenie zákonnosti spracúvania musí prevádzkovateľ vždy ponúkať náhradný spôsob prístupu do budovy bez spracúvania biometrických údajov, napr. pomocou preukazov [badges] alebo kľúčov.

78.

79. V takomto type prípadov, keď sa vytvárajú biometrické vzory, musia prevádzkovatelia zabezpečiť, že keď systém zistí zhodu, alebo naopak zhodu nepotvrdí, okamžite a bezpečným spôsobom sa odstránia všetky „medzivzory“, ktoré systém (s výslovným a informovaným súhlasom dotknutej osoby) počas danej relácie vyhotovil s cieľom porovnať ich so vzormi vytvorenými dotknutou osobou pri registrácii. Vzory vytvorené na registráciu by sa mali zachovať len na splnenie účelu spracúvania a nemali by sa uchovávať ani archivovať.

80. V prípade, že účelom spracúvania je napríklad rozlíšenie jednej kategórie ľudí od druhej, ale nie jedinečne niekoho identifikovať, takéto spracúvanie nepatrí do rozsahu pôsobnosti článku 9.

Príklad: Majiteľ obchodu by chcel zacieliť svoju reklamu na základe charakteristík týkajúcich sa pohlavia a veku zákazníkov zachytených systémom na monitorovanie kamerou. Ak toto zariadenie nevytvára biometrické vzory na účely jedinečnej identifikácie osôb, ale namiesto toho zachytáva ich fyzické charakteristiky na účely klasifikácie osoby, takéto spracúvanie by nepatrilo do rozsahu pôsobnosti článku 9 (pokiaľ sa nespracúvajú žiadne ďalšie typy osobitných kategórií údajov).

81.

82. Článok 9 sa však uplatňuje, ak prevádzkovateľ biometrické údaje uchováva [najčastejšie prostredníctvom vzorov vytvorených extrahovaním kľúčových prvkov z nespracovanej podoby biometrických údajov (napr. meranie tváre na základe snímky)] na jedinečnú identifikáciu osoby. Ak chce prevádzkovateľ zachytiť dotknutú osobu, ktorá opätovne vstupuje do daného priestoru alebo iného priestoru (napríklad s cieľom naplánovať pokračujúcu cielenú reklamu), potom by účelom bolo jedinečne identifikovať fyzickú osobu, čo znamená, že táto činnosť by od začiatku patrila do rozsahu pôsobnosti článku 9. Takýto prípad by mohol nastať, keď prevádzkovateľ uchováva vytvorené vzory na poskytovanie ďalšej prispôsobenej reklamy na niekoľkých bilbordoch rozmiestnených vo vnútri

predajne. Keďže systém používa fyzické charakteristiky na zachytenie konkrétnych osôb opätovne vstupujúcich do záberu kamery (napr. návštevníkov nákupného centra) a sleduje ich, predstavuje to metódu biometrickej identifikácie, pretože sa zameriava na rozpoznávanie pomocou osobitného technického spracúvania.

> Príklad: Majiteľ predajne nainštaloval systém na rozpoznávanie tvárí v predajni na účely prispôsobenia reklamy jednotlivcom. Prevádzkovateľ musí pred použitím takéhoto biometrického systému a poskytovaním prispôsobenej reklamy získať výslovný a informovaný súhlas všetkých dotknutých osôb. Ak by systém zaznamenával návštevníkov alebo okoloidúcich, ktorí nedali súhlas na vytvorenie biometrického vzoru, bol by nezákonný napriek tomu, že by sa ich vzor vymazal v čo najkratšej možnej lehote. Tieto dočasné vzory totiž predstavujú spracúvané biometrické údaje na účely jedinečnej identifikácie osoby, ktorá nemusí chcieť dostávať cielenú reklamu.

83.

84. EDPB poznamenáva, že niektoré biometrické systémy sú nainštalované v nekontrolovanom prostredí[17], čo znamená, že systém vyžaduje priebežné zachytávanie tvárí každej osoby prechádzajúcej v dosahu záberu kamery vrátane osôb, ktoré neposkytli súhlas s takýmto biometrickým zariadením, a tak vytvárajú biometrické vzory. Tieto vzory možno porovnať s vytvorenými vzormi dotknutých osôb, ktoré počas postupu registrácie poskytli predchádzajúci súhlas (t. j. používateľ biometrického zariadenia) na to, aby prevádzkovateľ rozlíšil, či je osoba používateľom biometrického zariadenia alebo nie. V tomto prípade je systém často nastavený tak, aby rozlišoval jednotlivcov, ktorých chce rozpoznať podľa databázy, od tých, ktorí registrovaní nie sú. Keďže účelom je jednoznačne identifikovať fyzické osoby, v prípade každej osoby zachytenej kamerou sa stále vyžaduje, aby sa uplatňovala výnimka podľa článku 9 ods. 2.

> Príklad: Hotel používa monitorovanie kamerou na automatické upozornenie manažéra hotela, že prišiel VIP hosť, a to na základe rozpoznania jeho tváre. Takýto VIP hosť predtým, ako bol zaevidovaný v databáze zriadenej na daný účel, poskytol výslovný predchádzajúci súhlas s používaním systému na rozpoznávanie tvárí. Takéto systémy na spracúvanie biometrických údajov by boli nezákonné, pokiaľ všetci ostatní monitorovaní hostia (za účelom identifikovania VIP hostí) neudelili súhlas so spracúvaním podľa článku 9 ods. 2 písm. a) všeobecného nariadenia o ochrane údajov.
>
> Príklad: Prevádzkovateľ nainštaluje pri vchode do koncertnej sály, ktorú spravuje, systém na monitorovanie kamerou s rozpoznávaním tvárí. Prevádzkovateľ musí jasne pripraviť oddelené vstupy: jeden s biometrickým systémom a jeden bez neho (kde sa naskenujú lístky). Vstupy vybavené biometrickými zariadeniami musia byť nainštalované a sprístupnené spôsobom, ktorý neumožňuje systému zachytávať biometrické vzory divákov, ktorí neposkytli súhlas.

85.

86. Ďalej treba uviesť, že ak sa v súlade s článkom 9 všeobecného nariadenia o ochrane údajov vyžaduje súhlas, prevádzkovateľ nesmie prístup k svojim službám podmieniť vyjadrením súhlasu so spracúvaním biometrických údajov. Inými slovami, a najmä v prípade, že sa biometrické údaje spracúvajú na účely overenia totožnosti [authentication purpose], prevádzkovateľ musí ponúknuť náhradné riešenie, ktoré

[17] Znamená to, že biometrické zariadenie je umiestnené v priestore, ktorý je otvorený pre verejnosť, a môže byť použité v prípade každého okoloidúceho človeka na rozdiel od biometrických systémov v kontrolovaných prostrediach, ktoré možno použiť len so zapojením osoby udeľujúcej súhlas.

nezahŕňa spracúvanie biometrických údajov, a to bez obmedzení alebo ďalších nákladov pre dotknutú osobu. Toto náhradné riešenie je takisto potrebné pre osoby, na ktoré sa vzťahujú obmedzenia použitia biometrického zariadenia (napr. nie je možné vykonať registráciu, resp. nasnímanie biometrických údajov, použitie je sťažené zdravotným postihnutím a pod.), a pre prípad predpokladanej nedostupnosti biometrického zariadenia (napr. poruchy zariadenia) musí byť pripravené „záložné riešenie“ na zabezpečenie kontinuálneho poskytovania ponúkanej služby, pričom sa však toto záložné riešenie použije len vo výnimočných prípadoch. Vo výnimočných prípadoch môže dôjsť k situácii, keď je spracúvanie biometrických údajov hlavnou činnosťou v rámci služby poskytovanej na základe zmluvy, napr. v prípade múzea, ktoré pripraví výstavu na predvedenie používania zariadenia na rozpoznávanie tvárí, pričom v takomto prípade dotknuté osoby nebudú môcť odmietnuť spracúvanie biometrických údajov, ak sa rozhodnú výstavu navštíviť. V takomto prípade je súhlas požadovaný článkom 9 stále platný, ak sú splnené požiadavky čl. 7.

5.2 Odporúčané opatrenia na minimalizáciu rizík pri spracúvaní biometrických údajov

87. V súlade so zásadou minimalizácie údajov musia prevádzkovatelia zabezpečiť, aby údaje získané z digitálnej snímky na účely vyhotovenia vzoru neboli neprimerané a obsahovali len informácie požadované na konkrétny účel, čím sa predíde možnému ďalšiemu spracúvaniu. Mali by sa zaviesť opatrenia, ktoré zaistia, že sa vzory nebudú môcť prenášať medzi biometrickými systémami.

88. Na identifikáciu a jej potvrdenie [authentication] / overenie [verification] sa pravdepodobne bude vyžadovať ukladanie vzorov na neskoršie porovnávanie. Prevádzkovateľ musí zvážiť najvhodnejšie miesto na ukladanie údajov. V kontrolovanom prostredí (napr. oddelené chodby alebo kontrolné miesta) by sa vzory mali ukladať v samostatnom zariadení v držbe používateľa a pod jeho výhradnou kontrolou (v smartfóne alebo na identifikačnej karte) alebo – ak sú potrebné na osobitné účely a pri existencii objektívnych potrieb – mali by sa uchovávať v centrálnej databáze v zašifrovanej forme, pričom kľúč/tajný kód na rozšifrovanie by mala mať k dispozícii len táto osoba, aby sa predišlo neoprávnenému prístupu k vzorom alebo k miestu uchovávania. Ak prevádzkovateľ nemôže zabrániť tomu, aby mal prístup ku vzorom, musí podniknúť vhodné kroky na zaistenie bezpečnosti uchovávaných údajov. Môže to zahŕňať zašifrovanie vzorov pomocou kryptografického algoritmu.

89. V každom prípade by prevádzkovateľ mal prijať všetky potrebné preventívne opatrenia, aby sa zachovala dostupnosť, integrita a dôvernosť spracúvaných údajov. V tejto súvislosti by prevádzkovateľ mal predovšetkým vykonať tieto opatrenia: rozdeliť údaje počas prenosu a uchovávania, uchovávať biometrické vzory a surové údaje [raw data] alebo údaje o identite v rôznych databázach, zašifrovať biometrické údaje, najmä biometrické vzory, a vymedziť systém šifrovania a správy kľúčov, zaviesť organizačné a technické opatrenia na odhaľovanie podvodov, pripojiť k údajom integračný kód [integrity code] (napr. podpis alebo hash) a zakázať prístup k biometrickým údajom zvonku. Takéto opatrenia sa budú musieť prispôsobovať v závislosti od vývoja technológií.

90. Okrem toho by prevádzkovatelia mali surové údaje [raw data] vymazávať (snímky tváre, znaky reči, chôdzu atď.) a zabezpečiť účinnosť vymazania. Ak už prestal existovať oprávnený základ na spracúvanie, surové údaje [raw data] musia byť vymazané. Dokonca by sa dalo povedať, že keďže sa biometrické vzory odvodzujú práve z takýchto údajov, zriadenie databázy by mohlo predstavovať rovnako veľké alebo aj väčšie riziko (pretože biometrický vzor nie je vždy ľahké prečítať, keď neviete, ako bol naprogramovaný, no surové údaje [raw data] ako také predstavujú základný stavebný prvok na vytvorenie akéhokoľvek vzoru. V prípade, že by prevádzkovateľ musel tieto údaje ukladať, treba zvážiť metódy pridania šumu [noise-additive methods] (napr. vodotlač), aby sa znemožnilo vytvorenie vzoru. Prevádzkovateľ musí biometrické údaje a vzory vymazať aj v prípade neoprávneného prístupu do terminálu na snímanie a porovnávanie údajov [read-comparison terminal] alebo do úložného

servera a po skončení životnosti biometrického zariadenia vymazať všetky údaje, ktoré nie sú potrebné na ďalšie spracúvanie.

6 PRÁVA DOTKNUTEJ OSOBY

91. Vzhľadom na charakter spracúvania údajov pri používaní monitorovania kamerou je vhodné ďalej objasniť niektoré práva dotknutých osôb stanovené vo všeobecnom nariadení o ochrane údajov. Táto kapitola však neobsahuje vyčerpávajúce informácie, na spracúvanie osobných údajov prostredníctvom monitorovania kamerou sa uplatňujú všetky práva stanovené vo všeobecnom nariadení o ochrane údajov.

6.1 Právo na prístup

92. Dotknutá osoba má právo získať potvrdenie od prevádzkovateľa o tom, či sa jej osobné údaje spracúvajú alebo nie. V prípade monitorovania kamerovým systémom to znamená, že ak sa žiadne údaje nijakým spôsobom neukladajú ani neprenášajú po uplynutí momentu monitorovania v reálnom čase, prevádzkovateľ by mohol poskytnúť len informáciu, že sa žiadne osobné údaje už nespracúvajú (okrem všeobecných informácií podľa článku 13, pozri oddiel 7 – Požiadavky na transparentnosť a informačnú povinnosť). Ak sa však v čase žiadosti údaje stále spracúvajú (napr. ak sa údaje ukladajú alebo akýmkoľvek spôsobom priebežne spracúvajú), dotknutá osoba by mala získať prístup a informácie v súlade s článkom 15.

93. V súvislosti s právom na prístup sa však v niektorých prípadoch môžu uplatňovať viaceré obmedzenia.

- Článok 15 ods. 4 všeobecného nariadenia o ochrane údajov, nepriaznivé dôsledky na práva a slobody iných

94. Vzhľadom na to, že na rovnakom zázname z monitorovania kamerou môže byť zachytený ľubovoľný počet osôb, jeho zobrazenie by potom viedlo k ďalšiemu spracúvaniu osobných údajov ďalších dotknutých osôb. Ak dotknutá osoba požiada o kópiu materiálu (článok 15 ods. 3), mohlo by to mať nepriaznivé dôsledky na práva a slobody ďalších dotknutých osôb, ktoré sú v ňom tiež zachytené. Za účelom predísť takémuto účinku by mal prevádzkovateľ v niektorých prípadoch zvážiť neposkytnutie videozáznamu, na ktorom je možné identifikovať iné dotknuté osoby, a to z dôvodu rušivej povahy takéhoto videozáznamu. Ochrana práv tretích strán by sa nemala používať na odôvodnenie odopretia oprávnených nárokov na prístup jednotlivcov, v takýchto prípadoch by prevádzkovateľ mal zaviesť technické opatrenia na splnenie žiadosti na prístup (napr. editovať snímky alebo ich zakódovať [scrambling]). Prevádzkovatelia však nie sú povinní zaviesť takéto technické opatrenia, keď môžu inak zabezpečiť, že sú schopní odpovedať na žiadosť podľa článku 15 v rámci časovej lehoty uvedenej v článku 12 ods. 3.

- Článok 11 ods. 2 všeobecného nariadenia o ochrane údajov, prevádzkovateľ nie je schopný identifikovať dotknutú osobu

95. Ak sa vo videozázname nedajú vyhľadať osobné údaje (t. j. prevádzkovateľ by musel prejsť veľké množstvo uchovávaného materiálu, aby našiel príslušnú dotknutú osobu), prevádzkovateľ nemusí byť schopný dotknutú osobu identifikovať.

96. Z týchto dôvodov by dotknutá osoba (okrem identifikovania sa preukazom totožnosti alebo osobne) mala v žiadosti predkladanej prevádzkovateľovi uviesť kedy – v rámci primeraného časového obdobia v pomere k množstvu zaznamenaných dotknutých osôb – do monitorovaného priestoru vstúpila. Prevádzkovateľ by mal dotknutej osobe vopred oznámiť, aké údaje sú na splnenie žiadosti potrebné. Ak prevádzkovateľ vie preukázať, že dotknutú osobu nie je schopný identifikovať, zodpovedajúcim spôsobom o tom informuje dotknutú osobu, ak je to možné. V takomto prípade by prevádzkovateľ mal vo svojej odpovedi dotknutú osobu informovať o presnej

oblasti, v ktorej monitoruje, potvrdiť kamery, ktoré používa a pod., aby dotknutá osoba úplne porozumela tomu, aké osobné údaje sa o nej mohli spracúvať.

> Príklad: Ak dotknutá osoba požaduje kópiu svojich osobných údajov spracúvaných prostredníctvom monitorovania kamerovým systémom pri vchode do nákupného centra s 30 000 návštevníkmi za deň, dotknutá osoba by mala presnejšie uviesť, kedy prešla monitorovanou oblasťou, poskytnutím časového rámca približne jednej hodiny. Ak prevádzkovateľ materiál stále spracúva, kópiu kamerového záznamu by mal poskytnúť. Ak je v tom istom materiáli možné identifikovať ďalšie dotknuté osoby, túto časť materiálu je pred odovzdaním kópie dotknutej osobe, ktorá žiadosť predložila, potrebné anonymizovať (napr. rozmazaním kópie alebo jej častí).
>
> Príklad: Ak prevádzkovateľ automaticky vymazáva všetky záznamy napríklad do dvoch dní, takýto prevádzkovateľ po uplynutí dvoch dní nedokáže poskytnúť dotknutej osobe záznamy. Ak prevádzkovateľ dostane žiadosť o prístup po uplynutí týchto dvoch dní, mal by podľa toho informovať dotknutú osobu.

97.

- Článok 12 všeobecného nariadenia o ochrane údajov, neprimerané žiadosti

98. V prípade neprimeraných alebo zjavne neopodstatnených žiadostí dotknutej osoby môže prevádzkovateľ buď požadovať primeraný poplatok v súlade s článkom 12 ods. 5 písm. a) všeobecného nariadenia o ochrane údajov, alebo môže odmietnuť konať na základe žiadosti [článok 12 ods. 5 písm. b) všeobecného nariadenia o ochrane údajov]. Zjavnú neopodstatnenosť alebo neprimeranosť žiadosti musí prevádzkovateľ vedieť preukázať.

6.2 Právo na vymazanie a právo namietať

6.2.1 Právo na vymazanie (právo na zabudnutie)

99. Ak prevádzkovateľ pokračuje v spracúvaní osobných údajov nad rámec monitorovania v reálnom čase (napr. v prípade uchovávania), dotknutá osoba môže požiadať o vymazanie osobných údajov podľa článku 17 všeobecného nariadenia o ochrane údajov.

100. Na základe žiadosti je prevádzkovateľ povinný osobné údaje bez zbytočného odkladu vymazať, ak sa uplatňuje jedna z okolností uvedených v článku 17 ods. 1 všeobecného nariadenia o ochrane údajov (a zároveň sa neuplatňuje žiadna z výnimiek uvedených v článku 17 ods. 3 všeobecného nariadenia o ochrane údajov). Zahŕňa to povinnosť vymazať osobné údaje, ak už nie sú potrebné na účel, na ktorý boli pôvodne uchovávané, alebo ak je spracúvanie nezákonné (pozri aj *oddiel 8 –Lehoty uchovávania a povinnosť vymazania*). Okrem toho, by sa mali osobné údaje vymazať v závislosti od právneho základu ich spracúvania:

- *pokiaľ ide o súhlas*, keď sa súhlas odvolá (a neuplatňuje sa žiadny iný právny základ spracúvania),
- pokiaľ ide o *oprávnený záujem*:
  - keď si dotknutá osoba uplatní právo namietať *(pozri oddiel 6.2.2)* a neprevažujú žiadne závažné [compelling] oprávnené dôvody na spracúvanie alebo
  - keď dotknutá osoba v prípade priameho marketingu (vrátane profilovania) proti spracúvaniu namieta.

101. Na základe žiadosti podľa čl. 17 ods. 2 všeobecného nariadenia o ochrane údajov, musí prevádzkovateľ podniknúť primerané kroky, aby informoval ostatných prevádzkovateľov (ktorí predmetné osobné údaje aktuálne spracúvajú), ak prevádzkovateľ videozáznam zverejnil (napr. prostredníctvom vysielania alebo streamovania online). Primerané kroky by mali zahŕňať technické opatrenia so zreteľom na dostupnú technológiu a náklady na vykonanie opatrení. Prevádzkovateľ by mal podľa možnosti v súlade s článkom 19 všeobecného nariadenia o ochrane údajov oznámiť vymazanie osobných údajov všetkým osobám, ktorým boli osobné údaje predtým poskytnuté.

102. Okrem povinnosti vymazať osobné údaje na žiadosť dotknutej osoby, je prevádzkovateľ povinný podľa všeobecných zásad všeobecného nariadenia o ochrane údajov obmedziť uchovávanie osobných údajov (pozri *oddiel 8*).

103. V prípade monitorovania kamerou je vhodné podotknúť, že napríklad rozmazaním obrazu bez možnosti opätovného obnovenia osobných údajov, ktoré obraz predtým obsahoval, sa osobné údaje v súlade so všeobecným nariadením o ochrane údajov považujú za vymazané.

> Príklad: Obchod so zmiešaným tovarom má problémy s vandalizmom, ktorý sa týka najmä jeho exteriéru, a preto využíva monitorovanie kamerou, ktorá je umiestnená vonku nad vchodom priamo upevnená na stenách. Okoloidúci požiada o vymazanie svojich osobných údajov z momentu, keď popri obchode prechádzal. Prevádzkovateľ je povinný na žiadosť odpovedať bez zbytočného odkladu a najneskôr do jedného mesiaca. Keďže predmetný záznam už nespĺňa účel, na ktorý bol pôvodne uchovávaný (v čase, keď dotknutá osoba prechádzala popri obchode, nedošlo k vandalizmu), v čase žiadosti neexistuje žiadny oprávnený záujem na uchovávaní údajov, ktorý by prevážil nad záujmami dotknutých osôb. Prevádzkovateľ musí osobné údaje vymazať.

104.

6.2.2 Právo namietať

105. V prípade monitorovania kamerou založenom na *oprávnenom záujme* [článok 6 ods.1 písm. f) všeobecného nariadenia o ochrane údajov] alebo nevyhnutného na plnenie úloh realizovaných vo *verejnom záujme* [článok 6 ods. 1 písm. e) všeobecného nariadenia o ochrane údajov] má dotknutá osoba právo z dôvodov týkajúcich sa jej konkrétnej situácie – kedykoľvek – namietať voči spracúvaniu v súlade s článkom 21 všeobecného nariadenia o ochrane údajov. Pokiaľ prevádzkovateľ nepreukáže závažné [compelling] oprávnené dôvody, ktoré prevažujú nad právami a záujmami dotknutej osoby, spracúvanie údajov jednotlivca, ktorý vzniesol námietky, sa musí zastaviť. Prevádzkovateľ by mal byť povinný odpovedať na žiadosť dotknutej osoby bez zbytočného odkladu a najneskôr do jedného mesiaca.

106. V súvislosti s monitorovaním kamerou by sa táto námietka mohla vzniesť buď pri vstupe, v čase zdržiavania sa v monitorovanej oblasti, alebo po výstupe z monitorovanej oblasti. V praxi to znamená, že pokiaľ prevádzkovateľ nemá závažné [compelling] oprávnené dôvody, monitorovanie oblasti, kde by bolo možné identifikovať fyzické osoby, je zákonné iba vtedy, ak

(1) je prevádzkovateľ na požiadanie schopný okamžite kameru pri spracúvaní osobných údajov zastaviť alebo

(2) je monitorovaná oblasť tak podrobne obmedzená, že prevádzkovateľ dokáže zabezpečiť súhlas dotknutej osoby ešte pred vstupom do tejto oblasti, a nejde o oblasť, do ktorej má dotknutá osoba ako občan právo vstúpiť.

107. Cieľom týchto usmernení nie je určiť, čo sa považuje za *závažný* [compelling] oprávnený záujem (článok 21 všeobecného nariadenia o ochrane údajov).

108. Pri využívaní monitorovania kamerou na účely priameho marketingu má dotknutá osoba právo namietať proti spracúvaniu na základe vlastného uváženia, pretože právo namietať je v tomto kontexte absolútne (článok 21 ods. 2 a 3 všeobecného nariadenia o ochrane údajov).

> Príklad: Spoločnosť má problémy s narušením bezpečnosti vo vchode určenom pre verejnosť a na základe oprávneného záujmu využíva monitorovanie kamerou s cieľom zaznamenať osoby, ktoré do nej vstupujú nezákonne. Návštevník proti spracúvaniu svojich údajov prostredníctvom monitorovania kamerovým systémom namieta z dôvodov týkajúcich sa jeho konkrétnej situácie. Spoločnosť však v tomto prípade žiadosť odmieta s vysvetlením, že uložené záznamy sú potrebné z dôvodu prebiehajúceho interného vyšetrovania, a teda má závažné [compelling] oprávnené dôvody na pokračovaní v spracúvaní osobných údajov.

109.

7 POŽIADAVKY NA TRANSPARENTNOSŤ A INFORMAČNÚ POVINNOSŤ[18]

110. V európskych právnych predpisoch o ochrane údajov sa už dávno uplatňuje podmienka, že by si dotknuté osoby mali byť vedomé funkčného monitorovania kamerou. O monitorovaných miestach by mali byť podrobne informované.[19] V rámci všeobecného nariadenia o ochrane údajov sú všeobecné požiadavky na transparentnosť a informačnú povinnosť stanovené v článku 12 a nasledujúcich článkoch. Podrobnejšie informácie sú uvedené v „Usmerneniach k transparentnosti podľa nariadenia 2016/679 (WP260)“ pracovnej skupiny zriadenej podľa článku 29, ktoré 25. mája 2018 schválil EDPB. V súlade s WP260, odsekom 26, sa pri získavaní osobných údajov „[…] od dotknutej osoby monitorovaním (napr. využitím automatizovaných zariadení na získavanie údajov alebo softvéru na získavanie údajov, ako sú kamery […]“ uplatňuje článok 13 všeobecného nariadenia o ochrane údajov.

111. Vzhľadom na objem informácií, ktoré sa majú poskytnúť dotknutej osobe, prevádzkovatelia môžu využiť viacvrstvový prístup [layered approach], ak sa rozhodnú využiť kombináciu metód na to, aby zabezpečili transparentnosť (ods. 35 WP260; ods. 22 WP89). Pokiaľ ide o monitorovanie kamerou, najdôležitejšie informácie by mali byť zobrazené na samotnom varovnom označení (prvá vrstva), zatiaľ čo ďalšie povinné údaje sa môžu poskytnúť inými prostriedkami (druhá vrstva).

7.1 Informácie prvej vrstvy (varovné označenie)

112. Prvá vrstva predstavuje primárny spôsob, akým sa prevádzkovateľ prvýkrát spojí s dotknutou osobou. V tejto fáze môžu prevádzkovatelia použiť varovné označenie, na ktorom budú zobrazené príslušné informácie. Zobrazené informácie možno uvádzať v kombinácii s ikonou, s cieľom poskytnúť dobre viditeľným, zrozumiteľným a ľahko čitateľným spôsobom zmysluplný prehľad zamýšľaného spracúvania (článok 12 ods. 7 všeobecného nariadenia o ochrane údajov). Formát informácií by sa mal prispôsobiť konkrétnym miestam (ods. 22 WP89).

7.1.1 Umiestnenie varovného označenia

113. Informácie by mali byť umiestnené na takom mieste, aby dotknutá osoba mohla ľahko rozpoznať čo všetko je monitorované ešte pred vstupom do monitorovanej oblasti (približne na úroveň očí). Pokiaľ neexistujú pochybnosti o tom, ktoré oblasti sú predmetom monitorovania, a jednoznačne sa objasní kontext monitorovania, nie je potrebné odhaľovať polohu kamery (ods. 22 WP 89). Dotknutá osoba musí byť schopná odhadnúť, ktorá oblasť je zachytená kamerou, aby sa mohla monitorovaniu vyhnúť alebo v prípade potreby prispôsobiť svoje správanie.

7.1.2 Obsah prvej vrstvy

114. Informáciami prvej vrstvy (varovného označenia) by sa mali vo všeobecnosti oznamovať najdôležitejšie informácie, napr. podrobné informácie o účeloch spracúvania, totožnosti prevádzkovateľa a existencii práv dotknutej osoby, spolu s informáciami o najväčších dopadoch spracúvania.[20] Tie môžu zahŕňať napríklad oprávnené záujmy prevádzkovateľa (alebo tretej strany) a kontaktné údaje zodpovednej

[18] V rámci vnútroštátnych predpisov sa môžu uplatňovať osobitné požiadavky.

[19] Pozri WP859, stanovisko 4/2004 pracovnej skupiny zriadenej podľa článku 29 o spracúvaní osobných údajov na základe monitorovania kamerou.

[20] Pozri ods. 38 WP260.

osoby (ak je to relevantné). Musia obsahovať aj odkaz na podrobnejšie informácie druhej vrstvy a kde a ako ich nájsť.

115. Okrem toho by označenie malo obsahovať aj všetky informácie, ktoré by mohli dotknutú osobu zaskočiť (ods. 38 WP260). Mohlo by ísť napríklad o prenosy tretím stranám, najmä ak sa nachádzajú mimo EÚ a lehotu uchovávania. Ak takéto informácie nie sú uvedené, dotknutá osoba by mala mať možnosť veriť, že sa monitoruje iba naživo (bez zaznamenávania údajov alebo prenosu tretím stranám).

116.

Príklad (nezáväzný návrh):

Monitorovanie kamerou!

Ďalšie informácie sú k dispozícii:
- v oznámení,
- na recepcii/prostredníctvom informácií pre zákazníkov/v registri,
- na internete (URL).

Totožnosť prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa:

Kontaktné údaje vrátane údajov prípadnej zodpovednej osoby:

Informácie o spracúvaní, ktoré majú najväčší vplyv na dotknutú osobu (napr. doba uchovávania alebo monitorovanie naživo, zverejňovanie alebo prenášanie videozáznamu tretím stranám):

Účel(-y) monitorovania kamerou:

Práva dotknutých osôb: Ako dotknutá osoba si môžete uplatniť viaceré práva, predovšetkým právo požiadať prevádzkovateľa o prístup k Vašim osobným údajom alebo právo na ich vymazanie.

Ďalšie informácie o monitorovaní kamerou, ktoré zahŕňajú aj Vaše práva, nájdete v úplných informáciách poskytovaných prevádzkovateľom prostredníctvom možností uvedených vľavo.

7.2 Informácie druhej vrstvy

117. Aj informácie druhej vrstvy sa musia dotknutej osobe sprístupniť na ľahko prístupnom mieste, napríklad v podobe úplného informačného listu, ktorý je k dispozícii na centrálnom mieste (napr. informačný pult, recepcia alebo pokladňa), alebo by mali byť zobrazené na jednoducho prístupnom plagáte. Ako už bolo uvedené, varovné označenie s informáciami prvej vrstvy musí obsahovať jasný odkaz na informácie druhej vrstvy. Okrem toho by bolo najlepšie, keby informácie prvej vrstvy obsahovali odkaz na digitálny zdroj (napr. QR kód alebo adresa webového sídla) informácií druhej vrstvy. Informácie by však mali byť ľahko dostupné aj v nedigitálnej podobe. Prístup k informáciám druhej vrstvy by mal byť možný aj bez vstupu do monitorovanej oblasti, najmä ak sú informácie poskytované digitálne (to sa dá dosiahnuť napríklad hypertextovým odkazom). Ďalším vhodným prostriedkom by mohlo byť telefónne číslo, na ktoré sa dá zavolať. Nech už sa informácie poskytujú akokoľvek, musia obsahovať všetko, čo je podľa článku 13 všeobecného nariadenia o ochrane údajov povinné.

118. Okrem týchto možností, a aby boli čo najúčinnejšie, EDPB podporuje využívanie technologických prostriedkov na poskytovanie informácií dotknutým osobám. Môžu zahŕňať napríklad geolokalizačné kamery a vrátane informácií z mapovacích aplikácií alebo webových sídel, aby jednotlivci mohli na jednej strane ľahko identifikovať a špecifikovať zdroje videa v súvislosti s uplatnením svojich práv a na druhej strane získať podrobnejšie informácie o spracovateľskej operácii.

Príklad: Majiteľ obchodu monitoruje svoj obchod. Na dosiahnutie súladu s článkom 13 stačí na ľahko viditeľné miesto pri vstupe do jeho obchodu umiestniť varovné označenie, ktoré obsahuje informácie prvej vrstvy. Okrem toho musí na pokladni alebo akomkoľvek inom centrálnom a ľahko prístupnom mieste vo svojom obchode poskytovať zoznam informácií obsahujúci informácie druhej vrstvy.

119.

8 LEHOTY UCHOVÁVANIA A POVINNOSŤ VYMAZANIA

120. Osobné údaje sa nesmú uchovávať dlhšie, než je potrebné na účely, na ktoré sa osobné údaje spracúvajú [článok 5 ods. 1 písm. c) a e) všeobecného nariadenia o ochrane údajov]. V niektorých členských štátoch sa v súvislosti s monitorovaním kamerou môžu na lehoty uchovávania vzťahovať špecifické ustanovenia v súlade s článkom 6 ods. 2 všeobecného nariadenia o ochrane údajov.

121. Či je alebo nie je nevyhnutné ukladať osobné údaje by sa malo riadiť obmedzeným časovým horizontom. Vo všeobecnosti, oprávnenými účelmi pre monitorovanie kamerou sú často ochrana majetku alebo uchovávanie dôkazov. Vzniknuté škody sa zvyčajne dajú preukázať do jedného alebo dvoch dní. Na uľahčenie preukázania súladu s rámcom ochrany údajov, je v záujme prevádzkovateľa vykonať organizačné opatrenia vopred (napr. v prípade potreby vymenuje zástupcu pre preverovanie a zabezpečovanie videomateriálu). Pri zohľadnení zásad článku 5 ods. 1 písm. c) a e) všeobecného nariadenia o ochrane údajov, konkrétne minimalizácie údajov a minimalizácie uchovávania, by sa osobné údaje mali vo väčšine prípadov (napr. na účel odhalenia vandalizmu) vymazať, v ideálnom prípade automaticky po niekoľkých dňoch. Čím je stanovená lehota uchovávania dlhšia (najmä ak presahuje 72 hodín), tým viac zdôvodnení oprávnenosti účelu a nutnosti uchovávania treba poskytnúť. Ak prevádzkovateľ nepoužíva monitorovanie kamerou iba na monitorovanie svojich priestorov, ale má v úmysle údaje aj uchovávať, musí zabezpečiť, aby bolo uchovávanie skutočne potrebné na naplnenie daného účelu. Ak je to tak, lehota uchovávania musí byť jasne vymedzená a individuálne stanovená pre každý účel samostatne. Za vymedzenie lehoty uchovávania v súlade so zásadami nevyhnutnosti a primeranosti a za preukázanie súladu s ustanoveniami všeobecného nariadenia o ochrane údajov zodpovedá prevádzkovateľ.

> Príklad: Majiteľ malého obchodu si vandalizmus obyčajne všimne ešte v ten istý deň. Dôsledkom čoho je, že bežná lehota uchovávania 24 hodín je dostačujúca. Víkendy, keď je obchod zatvorený, alebo dlhšia dovolenka môžu byť dôvodom na predĺženie lehoty uchovávania. Ak zistí škodu, takisto môže byť potrebné uchovávať videozáznam počas dlhšieho obdobia, aby mohol podniknúť právne kroky proti páchateľovi.

122.

9 TECHNICKÉ A ORGANIZAČNÉ OPATRENIA

123. Ako je uvedené v článku 32 ods. 1 všeobecného nariadenia o ochrane údajov, spracúvanie osobných údajov počas monitorovania kamerou musí byť nielen právom dovolené, ale prevádzkovatelia aj sprostredkovatelia ho musia primerane zabezpečiť. Vykonané **organizačné a technické opatrenia** musia byť **primerané rizikám pre práva a slobody fyzických osôb**, ktoré sú dôsledkom náhodného alebo nezákonného zničenia, straty, zmeny, neoprávneného poskytnutia údajov získaných prostredníctvom monitorovania kamerou alebo prístupu k nim. Podľa článkov 24 a 25 všeobecného nariadenia o ochrane údajov musia prevádzkovatelia prijať technické a organizačné opatrenia, a to aj s cieľom zabezpečiť dodržiavanie všetkých zásad ochrany údajov počas spracúvania, ako aj určiť prostriedky na uplatnenie práv dotknutých osôb vymedzených v článkoch 15 až 22 všeobecného nariadenia o ochrane údajov. Prevádzkovatelia by mali prijať interný rámec a politiky, aby zabezpečili takúto implementáciu opatrení v čase určovania prostriedkov spracúvania, ako aj v čase samotného spracúvania, vrátane vykonania posúdenia vplyvu na ochranu osobných údajov, ak je to potrebné.

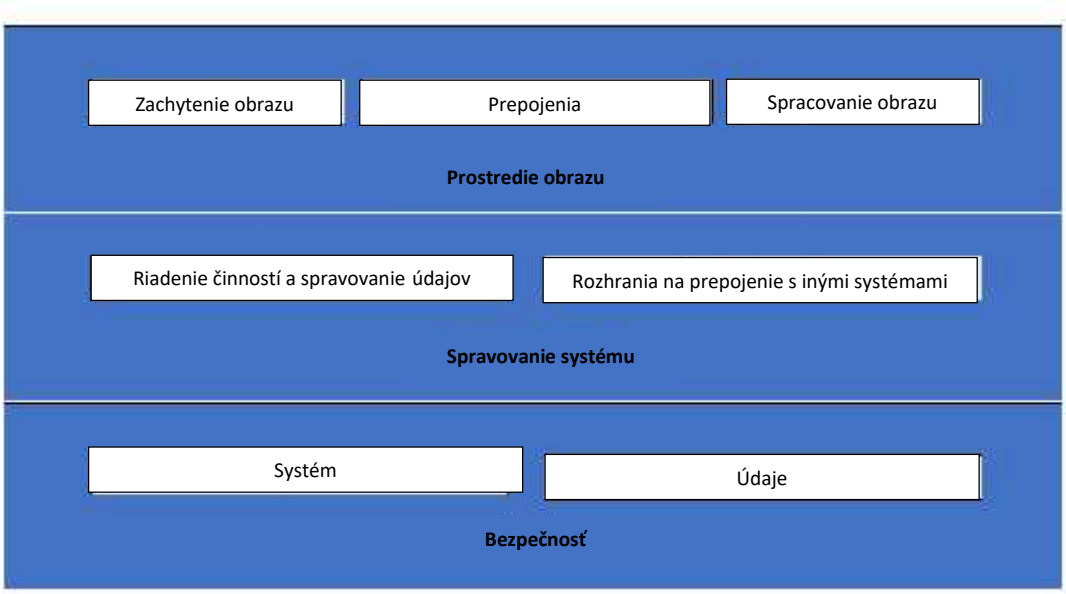
9.1 Prehľad systému na monitorovanie kamerou

124. Systém na monitorovanie kamerou[21] tvoria analógové a digitálne zariadenia spolu so softvérom na účely zachytávania snímok obrazu, spracovanie snímok a ich zobrazovanie operátorovi. Jeho súčasti sa rozdeľujú do týchto kategórií:

- Prostredie obrazu: zachytávanie snímok, prepojenia a spracovanie snímok:
  - účelom zachytávania snímok je vytvorenie obrazu skutočného sveta vo formáte, ktorý môže byť použitý zvyškom zariadenia,
  - prepojenia predstavujú kompletný prenos údajov v rámci prostredia obrazu, t. j. pripojenia a komunikáciu. Príkladmi prepojení sú káble, digitálne siete a bezdrôtové prenosy. Komunikáciu predstavujú všetky obrazové a kontrolné dátové signály, ktoré môžu byť digitálne alebo analógové.
  - spracovanie snímok zahŕňa analýzu, ukladanie a zobrazovanie snímky alebo sekvencie snímok.
- Z hľadiska riadenia systému má zariadenie na monitorovanie kamerovým systémom tieto logické funkcie:
  - spravovanie údajov a riadenie činností, ktoré zahŕňa spracovanie príkazov operátora a činnosti generované systémom (výstražný systém, upozornenia pre operátorov),
  - rozhrania na prepojenie s inými systémami môžu zahŕňať pripojenie k iným bezpečnostným (systém kontroly prístupu, požiarny poplachový systém) a iným ako bezpečnostným systémom (systémy riadenia budov, automatické rozpoznávanie tabuliek s evidenčným číslom vozidla),
- Bezpečnosť zariadenia na monitorovanie kamerovým systémom pozostáva z dôvernosti, integrity a dostupnosti systému a údajov:
  - bezpečnosť zariadenia zahŕňa fyzickú bezpečnosť všetkých zložiek a kontrolu prístupu k zariadeniu na monitorovanie,
  - bezpečnosť údajov zahŕňa prevenciu straty údajov a manipulácie s nimi.

[21] Všeobecné nariadenie o ochrane údajov nestanovuje vymedzenie tohto pojmu, technický opis možno nájsť napr. v norme EN 62676-1-1:2014 Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách – Časť 1-1: Požiadavky na obrazové systémy.

125.



Obrázok 1 – systém na monitorovanie kamerou

9.2 Špecificky navrhnutá a štandardná ochrana údajov [Data protection by design and by default]

126. Ako je uvedené v článku 25 všeobecného nariadenia o ochrane údajov, prevádzkovatelia musia prijať primerané technické a organizačné opatrenia na ochranu údajov v čase plánovania monitorovania kamerou, teda predtým, ako začnú získavať a spracúvať videozáznam. V týchto zásadách sa zdôrazňuje nevyhnutnosť zabudovaných technológií zvyšujúcich ochrany súkromia [privacy enhancing technologies], štandardné nastavenia na minimalizáciu spracúvania údajov a zabezpečenia potrebných nástrojov na umožnenie čo najvyššej ochrany osobných údajov[22].

127. Prevádzkovatelia by mali začleniť záruky na ochranu údajov a súkromia nielen do navrhovaných technologických špecifikácií, ale aj do organizačných postupov. Pokiaľ ide o organizačné postupy, prevádzkovateľ by mal v súvislosti s monitorovaním kamerou prijať vhodný rámec riadenia, ako aj prijať a presadzovať príslušné politiky a postupy. Z technického hľadiska by systémové špecifikácie a návrhy mali zahŕňať požiadavky na spracúvanie osobných údajov v súlade so zásadami uvedenými v článku 5 všeobecného nariadenia o ochrane údajov (zákonnosť spracúvania, obmedzenie účelu a údajov, štandardná minimalizácia údajov v zmysle článku 25 ods. 2 všeobecného nariadenia o ochrane údajov, integrita a dôvernosť, zodpovednosť atď.). Ak prevádzkovateľ plánuje obstarať komerčný kamerový monitorovací systém, musí tieto požiadavky zahrnúť do špecifikácií nákupu. Prevádzkovateľ musí zaistiť dodržiavanie týchto požiadaviek a uplatňovať ich na všetky zložky systému a na všetky údaje, ktoré spracúva, a to počas celého ich životného cyklu.

9.3 Konkrétne príklady príslušných opatrení

128. Väčšina opatrení, ktoré možno použiť na zaistenie bezpečnosti monitorovania kamerou, najmä ak sa používa digitálne vybavenie a softvér, sa nelíši od opatrení používaných v iných informačných

[22] WP 168, Stanovisko s názvom „Budúcnosť súkromia“, spoločný príspevok pracovnej skupiny pre ochranu súkromia zriadenej podľa článku 29 a pracovnej skupiny pre policajnú a justičnú spoluprácu ku konzultácii Európskej komisie vo veci právneho rámca pre základné právo na ochranu osobných údajov (prijaté 1. decembra 2009).

systémoch. Bez ohľadu na zvolené riešenie, prevádzkovateľ musí primerane chrániť všetky zložky systému na monitorovanie kamerou a údaje vo všetkých fázach, t. j. počas uchovávania (údaje v pokoji), prenosu (prenášané údaje) a spracúvania (používané údaje). Preto je potrebné, aby prevádzkovatelia a sprostredkovatelia skombinovali tak organizačné, ako aj technické opatrenia.

129. Pri výbere technických riešení by prevádzkovatelia mali zvážiť technológie, ktoré vo väčšej miere zohľadňujú ochranu súkromia, a to aj vzhľadom na to, že zvyšujú bezpečnosť. Príkladmi takýchto technológií sú systémy, ktoré umožňujú maskovanie a zakódovanie [scrambling] miest, ktoré nie sú pre monitorovanie relevantné, alebo vystrihnutie snímok tretích osôb pred poskytnutím videozáznamu dotknutým osobám.[23] Na druhej strane by vybraté riešenia nemali poskytovať funkcie, ktoré nie sú potrebné (napr. neobmedzený pohyb kamier, funkcia približovania, rádiový prenos, analyzovanie a zvukové nahrávanie). Poskytované funkcie, ktoré nie sú potrebné, sa musia deaktivovať.

130. K tejto téme je k dispozícii veľké množstvo literatúry, vrátane medzinárodných noriem a technických špecifikácií, týkajúcich sa fyzickej bezpečnosti multimediálnych systémov[24] a bezpečnosti všeobecných informačných systémov[25]. Tento oddiel preto poskytuje iba stručný prehľad najdôležitejších ustanovení tejto problematiky.

9.3.1 Organizačné opatrenia

131. Okrem prípadnej potreby vykonať posúdenie vplyvu na ochranu údajov (pozri *oddiel 10*) by prevádzkovatelia pri vytváraní vlastných politík a postupov týkajúcich sa monitorovania kamerou mali určiť aj:

- kto je zodpovedný za riadenie a fungovanie systému na monitorovanie kamerou,
- účel a rozsah projektu monitorovania kamerou,
- vhodné a zakázané používanie (kde a kedy je monitorovanie kamerou povolené resp. zakázané, napr. používanie skrytých kamier a nahrávanie nielen obrazu, ale aj zvuku)[26],
- opatrenia týkajúce sa transparentnosti, ako sa uvádza v *oddiele 7 (Požiadavky na transparentnosť a informačnú povinnosť,*
- ako sa obraz nahráva a počas akého časového obdobia vrátane archívneho uchovávania videozáznamov v súvislosti s bezpečnostnými incidentmi,
- kto musí absolvovať príslušnú odbornú prípravu a kedy,
- kto má prístup k videozáznamom a na aké účely,
- operačné postupy (napr. kto a odkiaľ sleduje monitorovanie kamerou, čo robiť v prípade incidentu porušenia ochrany údajov),
- aké postupy musia externé strany dodržať, ak chcú podať žiadosť o poskytnutie videozáznamov, ako aj postupy na zamietnutie a prijatie takýchto žiadostí,
- postupy týkajúce sa obstarávania, inštalácie a údržby zariadenia na monitorovanie kamerovým systémom,
- riadenie incidentov a obnova procesov.

---

[23] Na účely dodržiavania súladu s článkom 5 ods. 1 písm. c) môže byť používanie takýchto technológií v niektorých prípadoch dokonca povinné. V každom prípade však predstavujú príklady najlepších postupov.

[24] IEC TS 62045 – Bezpečnosť multimédií – Usmernenia týkajúce sa ochrany súkromia v prípade používaných zariadení a systémov a zariadení a systémov vyradených z používania.

[25] ISO/IEC 27000 – rad noriem týkajúcich sa systému riadenia informačnej bezpečnosti.

[26] Toto môže závisieť od vnútroštátnych a sektorových právnych predpisov.

9.3.2 Technické opatrenia

132. **Bezpečnosť systému** znamená **fyzickú bezpečnosť** všetkých zložiek systému a integritu systému, t. j. **ochrana a odolnosť proti úmyselnému a neúmyselnému zasahovaniu do bežnej prevádzky a kontrola prístupu.** Bezpečnosť údajov znamená **dôvernosť** (údaje dostupné len pre osoby, ktorým bol udelený prístup), **integritu** (predchádzanie strate údajov alebo manipulácie s nimi) a **dostupnosť** (v prípade potreby je prístup k údajom možný).

133. **Fyzická bezpečnosť** je nevyhnutnou súčasťou ochrany údajov a prvou obrannou líniou, pretože chráni zariadenie na monitorovanie kamerovým systémom pred krádežou, vandalizmom, prírodnou katastrofou, katastrofami spôsobenými ľudskou činnosťou a náhodným poškodením (napr. pred elektrickým prepätím, extrémnymi teplotami a rozliatou kávou). V prípade analógových zariadení má fyzická bezpečnosť pri ich ochrane hlavnú úlohu.

134. **Bezpečnosť systému a údajov**, t. j. ochrana pred úmyselným a neúmyselným zasahovaním do bežnej prevádzky, môže zahŕňať:

- ochranu kompletnej infraštruktúry zariadenia na monitorovanie kamerovým systémom (vrátane diaľkových kamier, kabeláže a zdroja napájania) pred fyzickou manipuláciou a krádežou,
- ochranu prenosu záznamu prostredníctvom komunikačných kanálov zabezpečených proti zachyteniu údajov,
- šifrovanie údajov,
- používanie riešení založených na hardvéri alebo softvéri, ako sú firewally, antivírusy alebo systémy na odhaľovanie narušenia proti kybernetickým útokom,
- zisťovanie porúch súčiastok, softvéru a prepojení,
- prostriedky na obnovenie dostupnosti osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu.

135. **Kontrolou prístupu** sa zabezpečuje, že k systému a údajom majú prístup len oprávnené osoby, pričom iným osobám sa v tom zabraňuje. Opatrenia na podporu kontroly fyzického a logického prístupu zahŕňajú:

- zabezpečenie, aby všetky priestory, ktoré sú monitorované kamerovým systémom, a v ktorých uchovávajú videozáznamy, boli zabezpečené pred nekontrolovaným prístupom tretích strán,
- umiestnenie monitorov takým spôsobom (najmä ak sú v otvorených priestoroch, ako je recepcia), aby ich videli len poverení operátori,
- vymedzenie a presadzovanie postupov na udeľovanie, zmenu a odvolanie fyzického alebo logického prístupu,
- zavedenie metód a prostriedkov na autentifikáciu [authentication] používateľov a ich overovanie [authorization] napr. prostredníctvom stanovenia dĺžky hesla a frekvencie jeho zmeny,
- zaznamenávanie a pravidelné preskúmanie operácií vykonaných používateľmi (v súvislosti so zariadením aj s údajmi),
- priebežné vykonávanie monitorovania a zisťovanie porúch prístupu a čo najskoršie riešenie identifikovaných slabých miest.

10 POSÚDENIE VPLYVU NA OCHRANU ÚDAJOV

136. Článok 35 ods. 1 všeobecného nariadenia o ochrane údajov ustanovuje, že ak typ spracúvania údajov pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ vykoná posúdenie vplyvu na ochranu osobných údajov. Článok 35 ods. 3 písm. c) všeobecného nariadenia o ochrane údajov sa stanovuje, že prevádzkovatelia sú povinní vykonať posúdenie vplyvu na ochranu údajov, ak spracúvanie predstavuje systematické monitorovanie verejne prístupných miest vo veľkom rozsahu. Okrem toho sa v zmysle článku 35 ods. 3 písm. b) všeobecného nariadenia o ochrane údajov vyžaduje posúdenie vplyvu na ochranu údajov, ak prevádzkovateľ plánuje spracúvať osobitné kategórie údajov vo veľkom rozsahu.

137. V usmerneniach týkajúcich sa posúdenia vplyvu na ochranu údajov[27] sú uvedené ďalšie odporúčania, ako aj podrobnejšie príklady v súvislosti s monitorovaním kamerou (napr. používanie kamerového systému na monitorovanie spôsobu jazdenia na diaľniciach). Článok 35 ods. 4 všeobecného nariadenia o ochrane údajov vyžaduje, aby každý dozorný orgán zverejnil zoznam tých spracovateľských operácií, ktoré v rámci jeho krajiny podliehajú požiadavke na posúdenie vplyvu na ochranu údajov. Tieto zoznamy zvyčajne možno nájsť na webových sídlach dozorných orgánov. Vzhľadom na typické účely monitorovania kamerou (ochrana ľudí a majetku, odhaľovanie, prevencia a kontrola trestných činov, získavanie dôkazov a biometrická identifikácia podozrivých) je primerané predpokladať, že v mnohých prípadoch monitorovania kamerou sa bude vyžadovať posúdenie vplyvu na ochranu údajov. Preto by sa prevádzkovatelia mali dôkladne oboznámiť s týmito dokumentmi, aby mohli určiť, či sa takéto posúdenie vyžaduje a v prípade potreby ho vykonali. Na základe výsledkov vykonaného posúdenia vplyvu na ochranu údajov prevádzkovateľ určí, aké opatrenia na ochranu údajov prijme.

138. Ďalej treba uviesť, že ak sa na základe výsledkov posúdenia vplyvu na ochranu údajov ukáže, že napriek bezpečnostným opatreniam, ktoré prevádzkovateľ plánuje, takéto spracúvanie povedie k vysokému riziku, pred spracúvaním údajov bude potrebné uskutočniť konzultácie s príslušným dozorným orgánom. Podrobné informácie o predchádzajúcich konzultáciách sa nachádzajú v článku 36.

Za Európsky výbor pre ochranu údajov

predsedníčka

(Andrea Jelinek)

[27] WP248 rev. 01, Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“ – schválené EDPB.