

**Usmernenia 3/2019 o spracúvaní osobných údajov prostredníctvom kamerových zariadení**

**Verzia 2.0**

**Schválené 29. januára 2020**

|  |  |
| --- | --- |
| Schválené | 1 |

História verzií

|  |  |  |  |
| --- | --- | --- | --- |
| Verzia 2.0 | 29 | . januára 2020 | Prijatie usmernení po verejnej konzultácii |
|  |  |  |  |
| Verzia 1.0 | 10 | . júla 2019 | Prijatie usmernení pre verejné konzultácie |
|  |  |  |  |

Schválené 2

**Obsah**

|  |  |  |
| --- | --- | --- |
| 1 | Úvod ................................................................................................................................................. | 5 |
| 2 | Pôsobnosť ........................................................................................................................................ | 7 |
|  | 2.1 | Osobné údaje ........................................................................................................................... | 7 |
|  | 2.2 | Uplatňovanie Smernice o presadzovaní práva, LED (EU2016/680) ......................................... | 7 |
|  | 2.3 | Výnimka pre domácnosti ......................................................................................................... | 7 |
| 3 | Zákonnosť spracovania .................................................................................................................... | 9 |
|  | 3.1 | Oprávnený záujem, článok 6 (1) (f) ......................................................................................... | 9 |
|  | 3.1.1 | Existencia oprávnených záujmov ..................................................................................... | 9 |
|  | 3.1.2 | Potreba spracovania ...................................................................................................... | 10 |
|  | 3.1.3 | Vyvažovanie záujmov ..................................................................................................... | 11 |
|  | 3.2 Nevyhnutnosť plniť úlohu vykonávanú vo verejnom záujme alebo pri výkone verejnej moci zverenej kontrolórovi, Článok 6 (1) (e) .............................................................................................. |  |
|  | 13 |
|  | 3.3 | Súhlas, Článok 6 (1) (a) ........................................................................................................... | 14 |
| 4 | Zverejňovanie videozáznamov tretím stranám .............................................................................. | 15 |
|  | 4.1 | Zverejňovanie videozáznamov tretím stranám vo všeobecnosti ........................................... | 15 |
|  | 4.2 | Zverejnenie videozáznamov orgánom činným v trestnom konaní ........................................ | 15 |
| 5 | Spracúvanie osobitných kategórií údajov ...................................................................................... | 17 |
|  | 5.1 | Všeobecné úvahy pri spracovávaní biometrických údajov .................................................... | 18 |
|  | 5.2 | Navrhované opatrenia na minimalizáciu rizík pri spracovaní biometrických údajov ............ | 21 |
| 6 | Práva dotknutej osoby ................................................................................................................... | 22 |
|  | 6.1 | Právo na prístup ..................................................................................................................... | 22 |
|  | 6.2 | Právo na výmaz a právo namietať .......................................................................................... | 23 |
|  | 6.2.1 | Právo na vymazanie (Právo byť zabudnutý) ................................................................... | 23 |
|  | 6.2.2 | Právo namietať ............................................................................................................... | 24 |
| 7 | Povinnosti týkajúce sa transparentnosti a informovania ............................................................... | 26 |
|  | 7.1 | Informácie prvej vrstvy (výstražné označenie) ....................................................................... | 26 |
|  | 7.1.1 | Umiestnenie výstražného označenia ............................................................................. | 26 |
|  | 7.1.2 | Obsah prvej vrstvy ......................................................................................................... | 26 |
|  | 7.2 | Informácie druhej vrstvy ........................................................................................................ | 27 |
| 8 | Obdobia uchovávania a povinnosť vymazania ............................................................................... | 28 |
| 9 | Technické a organizačné opatrenia ................................................................................................ | 28 |
|  | 9.1 | Prehľad systému video monitorovania .................................................................................. | 29 |
|  | 9.2 | Ochrana údajov podľa návrhu a podľa štandardu .................................................................. | 30 |
|  | 9.3 | Konkrétne príklady príslušných opatrení ............................................................................... | 30 |

Schválené 3

|  |  |  |  |
| --- | --- | --- | --- |
|  | 9.3.1 | Organizačné opatrenia ..................................................................................................... | 31 |
|  | 9.3.2 | Technické opatrenia ....................................................................................................... | 31 |
| 10 | Posúdenie vplyvu na ochranu údajov .......................................................................................... | 33 |

Schválené 4

**Európsky výbor pre ochranu údajov**

S ohľadom na článok 70 ods. 1 písm. e) nariadenia Európskeho parlamentu a Rady 2016/679/EÚ z 27. apríla 2016 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov a ktorou sa zrušuje Smernica 95/46/ES (ďalej len „GDPR“),

S ohľadom na Dohodu o EHP, a najmä na jej prílohu XI a protokol 37, zmenenou a doplnenou rozhodnutím Spoločného výboru EHP č. 154/2018 zo 6. júla 2018,

S ohľadom na článok 12 a článok 22 rokovacieho poriadku,

**Bolo schválené nasledujúce usmernenie**

* 1. ÚVOD
1. Intenzívne používanie video zariadení má vplyv na správanie občanov. Rozsiahle využívanie takýchto nástrojov v mnohých sférach života jednotlivca bude vyvíjať na jednotlivca ďalší tlak, aby sa zabránilo identifikovaniu niečoho, čo by sa mohlo vnímať ako anomália. Tieto technológie môžu v skutočnosti obmedziť možnosti anonymného pohybu a anonymného využívania služieb a vo všeobecnosti obmedziť možnosť zostať bez povšimnutia. Dôsledky na ochranu údajov sú tak obrovské.
2. Hoci jednotlivcom nemusí prekážať používanie video záznamov zriadených na určitý bezpečnostný účel, je potrebné prijať určité 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 v súčasnosti používa mnoho nástrojov na využívanie zachytených snímok a premenu tradičných kamier na inteligentné (smart) kamery. Množstvo údajov generovaných videom v kombinácii s týmito nástrojmi a technikami zvyšuje riziká sekundárneho použitia (či už súvisí alebo nesúvisí s účelom pôvodne prideleným systému) alebo dokonca riziko zneužitia. V súvislosti s video monitorovaním by sa mali preto vždy starostlivo zvážiť všeobecné zásady stanovené v GDPR (článok 5).
3. Systémy video v mnohých ohľadoch menia spôsob, akým odborníci zo súkromného a verejného sektora interagujú na súkromných alebo verejných miestach za účelom zvýšenia bezpečnosti, získania analýzy publika, poskytovania personalizovanej reklamy atď. Video monitorovanie sa stalo vysoko výkonným vďaka intenzívnejšej implementácii inteligentnej analýzy videa. Tieto techniky môžu byť intruzívne (napríklad komplexné biometrické technológie) alebo menej intruzívne (napr. jednoduché výpočtové algoritmy).

Zostať v anonymite a zachovať si súkromie je vo všeobecnosti čoraz ťažšie. Otázky ochrany údajov, ktoré vznikajú v každej situácii sa môžu líšiť, rovnako ako právna analýza pri použití jednej alebo druhej z týchto technológií.

1. Okrem problémov s ochranou súkromia existujú aj riziká spojené s možnými poruchami týchto zariadení a zaujatosť, ktorú môžu spôsobovať. Vedci uvádzajú, že softvér používaný na identifikáciu, rozpoznávanie alebo analýzu tváre funguje odlišne v závislosti od veku, pohlavia a etnicity osoby, ktorú identifikuje.
	1. Odkazy na „členské štáty“ uvedené v tomto stanovisku by sa mali chápať ako odkazy na „členské štáty EHP“.

Schválené 5

Algoritmy by tak mali fungovať na základe rôznych demografických údajov, a preto zaujatosť pri rozpoznávaní tváre môže predstavovať hrozbu tvorenia predsudkov v spoločnosti. Z tohto dôvodu musia správcovia údajov zabezpečiť, aby biometrické spracovanie údajov pochádzajúce z video monitorovania podliehalo pravidelnému hodnoteniu jeho relevantnosti a dostatočnosti poskytnutých záruk.

1. Video monitorovanie nie je zo zásady nevyhnutnosťou, ak existujú iné prostriedky na dosiahnutie jeho základného účelu. V opačnom prípade riskujeme zmenu v kultúrnych normách, ktorá povedie k akceptovaniu nedostatku súkromia ako všeobecnej normy.
2. Cieľom týchto usmernení je poskytnúť usmernenie o tom, ako uplatňovať GDPR vo vzťahu k spracovaniu osobných údajov prostredníctvom kamerových zariadení. Príklady tu uvedené nie sú vyčerpávajúce, všeobecné odôvodnenie sa môže uplatniť na všetky potenciálne oblasti použitia.

Schválené 6

2 PÔSOBNOSŤ2

2.1 Osobné údaje

1. Systematické automatizované monitorovanie konkrétneho priestoru optickými alebo audiovizuálnymi prostriedkami, väčšinou na účely ochrany majetku alebo na ochranu života a zdravia jednotlivca, sa stalo významným fenoménom našej doby. Táto činnosť vedie k zhromažďovaniu a uchovávaniu obrazových alebo audiovizuálnych informácií o všetkých osobách vstupujúcich do monitorovaného priestoru, ktoré sú identifikovateľné na základe ich vzhľadu alebo iných špecifických prvkov. Na základe týchto údajov sa môže zistiť totožnosť týchto osôb. To umožňuje aj ďalšie spracovanie osobných údajov v súvislosti s prítomnosťou a správaním osôb v danom priestore. Potenciálne riziko zneužitia týchto údajov sa zvyšuje vo vzťahu k rozmeru monitorovaného priestoru, ako aj k počtu osôb, ktoré tento priestor navštevujú. Táto skutočnosť sa odráža vo Všeobecnom nariadení o ochrane údajov v článku 35 ods. 3 písm. c), v ktorom sa vyžaduje vykonanie kontrolu a posúdenia vplyvu na ochranu údajov aj v prípade systematického monitorovania verejne prístupnej oblasti vo veľkom meradle, ako aj v článku 37 ods. 1 písm. b), v ktorom sa od spracovateľov vyžaduje, aby menovali zodpovednú osobu (DPO), ak operácia spracúvania z dôvodu svojej povahy vyžaduje pravidelné a systematické monitorovanie dotknutých osôb.
2. Toto nariadenie sa však nevzťahuje na spracovanie údajov, ktoré nemá žiadny odkaz na osobu, napr. ak jednotlivca nemožno priamo alebo nepriamo identifikovať.

Príklad: GDPR nie je použiteľné pre falošné kamery (t. j. všetky kamery, ktoré sú v skutočnosti nefunkčnými kamerami, a teda nespracúvajú žiadne osobné údaje). *V niektorých členských štátoch by však mohli podliehať iným právnym predpisom.*

Príklad: Záznamy z vysokých výšok spadajú do rozsahu pôsobnosti GDPR, iba ak sa za daných okolností môžu spracované údaje týkať konkrétnej osoby.

Príklad: Videokamera je integrovaná v aute na poskytovanie pomoci pri parkovaní. Ak je kamera skonštruovaná alebo nastavená takým spôsobom, že nezhromažďuje žiadne informácie týkajúce sa fyzickej osoby (ako sú ŠPZ alebo informácie, ktoré by mohli identifikovať okoloidúcich), GDPR sa neuplatňuje.

9.

2.2 Uplatňovanie Smernice o presadzovaní práva, LED (EU2016/680)

1. Smernica EU2016/680 sa vzťahuje najmä na spracúvanie osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo výkonu trestov vrátane ochrany a predchádzania ohrozeniam verejnej bezpečnosti.

2.3 Výnimka pre domácnosti

1. Podľa článku 2 ods. 2 písm. s) je spracúvanie osobných údajov fyzickou osobou v rámci čisto osobnej činnosti alebo činnosti v domácnosti, ktoré môže zahŕňať aj činnosť online, mimo rozsahu pôsobnosti GDPR.3
2. Toto ustanovenie – tzv. výnimka pre domácnosti – sa v súvislosti s kamerovým monitorovaním musí vykladať v úzkom význame. Podľa názoru Európskeho súdneho dvora sa takzvaná „výnimka pre domácnosť“ musí vykladať v tom zmysle, že sa týka:

2 EDPB poznamenáva, že ak to GDPR umožňuje, môžu sa vo vnútroštátnych právnych predpisoch uplatňovať osobitné požiadavky. 3 Pozri tiež Odôvodnenie 18.

Schválené 7

“*iba činností, ktoré sa vykonávajú v priebehu súkromného alebo rodinného života jednotlivcov, čo zjavne nie je prípad spracovania osobných údajov, ktoré spočíva v uverejnení na internete takým spôsobom, aby boli tieto údaje prístupné neobmedzenému počtu ľudí*”.4Okrem toho, pokiaľ ide o systém video monitorovania, do tej miery, do akej zahŕňa neustále zaznamenávanie a uchovávanie osobných údajov a zároveň zahŕňa, “*čo i len čiastočne, verejný priestor, a preto je nasmerovaný smerom von zo súkromného prostredia osoby, ktorá údaje spracúva týmto spôsobom, nemožno to považovať za činnosť, ktorá je čisto „osobnou alebo domácou“ činnosťou v zmysle článku 3 ods. 2 druhej zarážky smernice 95/46”*5.

1. Pokiaľ ide o video zariadenia prevádzkované v priestoroch súkromnej osoby, môžu spadať pod výnimku pre domácnosti. Závisí to od niekoľkých faktorov, ktoré je potrebné zvážiť, aby sa mohli vyvodiť príslušné závery. Okrem vyššie uvedených prvkov identifikovaných rozhodnutiami Európskeho súdneho dvora musí používateľ video monitorovania v domácnosti mať na zreteli aj to, či má nejaký osobný vzťah s dotknutou osobou, či rozsah alebo frekvencia monitorovania naznačuje nejakú odbornú činnosť týkajúcu sa jeho osoby a možného nepriaznivého vplyvu takéhoto monitorovania na dotknutú osobu. Prítomnosť niektorého z vyššie uvedených prvkov nemusí nevyhnutne naznačovať, že spracovanie nespadá do rozsahu výnimky pre domácnosti, na toto určenie je potrebné celkové posúdenie.

Príklad: Turista nahráva videá prostredníctvom mobilného telefónu a videokamery, aby si zdokumentoval svoju dovolenku. Zábery ukazuje priateľom a rodine, ale neumožňuje ich prístup pre neurčitý počet ľudí. To by spadalo pod výnimku pre domácnosti.

Príklad: Zjazdový horský cyklista chce zaznamenať svoj zostup pomocou akčnej kamery. Jazdí na odľahlom mieste a nahrávky plánuje používať iba pre svoju osobnú zábavu doma. To by spadalo pod výnimku pre domácnosti, aj keby sa do určitej miery spracovávali osobné údaje.

Príklad: Niekto monitoruje a zaznamenáva svoju vlastnú záhradu. Nehnuteľnosť je oplotená a do záhrady vstupuje pravidelne len prevádzkovateľ sám a jeho rodina. To by spadalo pod výnimku pre domácnosti za predpokladu, že video monitorovanie nepresahuje ani čiastočne na verejný priestor alebo na susedný majetok.

14.

1. Európsky súdny dvor, Rozsudok vo veci C-101/01, prípad Bodil Lindqvist, 6. novembra 2003, bod 47.
2. Európsky súdny dvor, Rozsudok vo veci C-212/13, *František Ryneš vs Úřad pro ochranu osobních údajů*, 11. decembra 2014, ods. 33.

Schválené 8

* 1. ZÁKONNOSŤ SPRACOVANIA
1. Pred použitím sa musia spresniť účely spracovania (článok 5 ods. 1 písm. b)). Video monitorovanie môže slúžiť na mnohé účely, napr. podpora ochrany nehnuteľnosti a iných majetkov, podpora ochrany života a fyzickej integrity jednotlivcov, zhromažďovanie dôkazov o občianskych nárokoch.6 Tieto monitorovacie účely by mali byť písomne zdokumentované (článok 5 ods. 2) a je potrebné ich špecifikovať pre každú použitú monitorovaciu kameru. Kamery, ktoré používa ten istý prevádzkovateľ na ten istý účel, sa môžu dokumentovať spoločne. Dotknuté osoby musia byť navyše informované o účele (účeloch) spracovania v súlade s článkom 13 (*pozri oddiel 7, Povinnosti týkajúce sa spracovania a informovania*). Video monitorovanie založené iba na „bezpečí“ alebo „pre vašu bezpečnosť“ nie je dostatočne špecifické (článok 5 ods. 1 písm. b)). Okrem toho je to v rozpore so zásadou, že osobné údaje sa v súvislosti s dotknutou osobou majú spracúvať zákonne, spravodlivo a transparentne [pozri článok 5 ods. 1 písm. a)].
2. Každý právny dôvod podľa článku 6 ods. 1 môže v zásade poskytnúť právny základ na spracovanie údajov pochádzajúcich z video monitorovania. Napríklad článok 6 ods. 1 písm. c) sa uplatňuje vtedy, keď vnútroštátne právne predpisy ustanovujú povinnosť vykonávať video monitorovanie.7 V praxi sa však budú používať nasledujúce ustanovenia:
	* + Článok 6 (1) (f) (oprávnený záujem),
		+ Článok 6 (1) (e) (nevyhnutnosť vykonať úlohu vykonávanú vo verejnom záujme alebo pri výkone verejnej moci).

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

3.1 Oprávnený záujem, článok 6 (1) (f)

1. Právne posúdenie článku 6 ods. 1 písm. f) by malo byť založené na nasledujúcich kritériách v súlade s Odôvodnením 47.

3.1.1 Existencia oprávnených záujmov

1. je zákonné, ak je to potrebné na splnenie účelu legitímneho záujmu, ktorý sleduje prevádzkovateľ alebo tretia strana, pokiaľ takéto záujmy nie sú potlačené záujmom alebo základnými právami a slobodami dotknutej osoby (článok 6 ods. 1 písm. f). Oprávnené záujmy, ktoré sleduje prevádzkovateľ alebo tretia strana, môžu byť zákonné8, hospodárske alebo nemateriálne záujmy.9 Prevádzkovateľ by však mal vziať do úvahy, že ak dotknutá osoba namieta proti monitorovaniu v súlade s článkom 21, prevádzkovateľ môže pokračovať s videom monitorovaním dotknutej osoby, iba ak je na to závažný oprávnený záujem, ktorý má prednosť pred záujmami, právami a slobodami dotknutej osoby alebo na účely určenia, výkonu alebo obrany právnych nárokov.
2. Pri existencii skutočnej a nebezpečnej situácie môže účel ochrany majetku proti vlámaniu, krádeži alebo vandalizmu predstavovať oprávnený záujem pre vykonávanie video monitorovania.

6 Pravidlá zhromažďovania dôkazov pre občianskoprávne nároky sa v jednotlivých členských štátoch líšia.

7 Tieto usmernenia neanalyzujú vnútroštátne právne predpisy, ktoré sa môžu medzi členskými štátmi líšiť, ani ich nepreskúmavajú.

8 Európsky súdny dvor, Rozsudok vo veci C-13/16, prípad *Rīgas satiksme*, 4. mája 2017 9 pozri WP217, článok 29 Pracovná skupina.

|  |  |
| --- | --- |
| Schválené | 9 |

1. Oprávnený záujem musí byť skutočne existovať a musí byť aktuálnou otázkou (t. j. nesmie byť fiktívny alebo špekulatívny)10. Pred spustením monitorovania musí byť k dispozícii krízová situácia v reálnom živote - napríklad škody alebo vážne incidenty v minulosti. Na základe zásady zodpovednosti by sa prevádzkovateľom odporúčalo zdokumentovať príslušné incidenty (dátum, spôsob, finančná strata) a súvisiace trestné oznámenia. Tieto zdokumentované incidenty môžu byť silným dôkazom existencie oprávneného záujmu. Existencia oprávneného záujmu, ako aj nevyhnutnosť monitorovania by sa mali prehodnocovať v pravidelných intervaloch (napr. raz ročne, v závislosti od okolností).

Príklad: Majiteľ obchodu chce otvoriť nový obchod a chce si tam nainštalovať monitorovací systém, aby zabránil vandalizmu. Poskytnutím štatistických údajov môže dokázať, že v blízkom okolí existuje vysoké riziko vandalizmu. Užitočné sú aj skúsenosti zo susedných obchodov. Nie je potrebné, aby došlo k poškodeniu predmetného prevádzkovateľa. Pokiaľ škody spôsobené v susedstve naznačujú nebezpečenstvo alebo niečo podobné, môžu indikovať oprávnený záujem. Nestačí však uviesť štatistiku o vnútroštátnej alebo všeobecnej trestnej činnosti bez analýzy dotknutej oblasti alebo nebezpečenstiev pre tento konkrétny obchod.

21.

1. Bezprostredné nebezpečné situácie môžu predstavovať oprávnený záujem, t.j. napríklad banky alebo obchody predávajúce drahocenný tovar (napríklad klenotníci) alebo oblasti, o ktorých je známe, že sú typickými pre výskyt trestných činov v majetkovej oblasti (napríklad čerpacie stanice).
2. GDPR tiež jasne uvádza, že verejné orgány nemôžu opierať svoje spracovanie na základe oprávneného záujmu, pokiaľ vykonávajú svoje úlohy, článok 6 ods. 1 veta 2.

3.1.2 Potreba spracovania

1. Osobné údaje by mali byť primerané, relevantné a obmedzené na to, čo je potrebné vzhľadom na účely, na ktoré sa spracúvajú („minimalizácia údajov“), pozri článok 5 ods. 1 písm. c). Pred inštaláciou systému video monitorovania by prevádzkovateľ mal vždy kriticky preskúmať, či je toto opatrenie v prvom rade vhodné na dosiahnutie požadovaného cieľa, a za druhé primerané a potrebné na jeho účely. Opatrenia týkajúce sa video monitorovania by sa mali zvoliť iba vtedy, ak účel spracovania nemohol byť primerane splnený inými prostriedkami, ktoré menej zasahujú do základných práv a slobôd dotknutej osoby.
2. Vzhľadom na situáciu, v ktorej chce prevádzkovateľ zabrániť trestným činom súvisiacim s majetkom, môže prevádzkovateľ namiesto inštalácie videozáznamu prijať aj alternatívne bezpečnostné opatrenia, ako je oplotenie majetku, zavedenie pravidelnej hliadky bezpečnostnými pracovníkmi, používanie strážnej služby, zavedenie lepšieho osvetlenia, inštalácia zabezpečovacieho systému, napr. bezpečnostné zámky, okná a dvere odolné voči neoprávnenému zásahu alebo nanášanie anti-graffiti náterov alebo fólií na steny. Tieto opatrenia môžu byť proti vlámaniu, krádeži a vandalizmu rovnako účinné ako systémy video monitorovania. Prevádzkovateľ musí od prípadu k prípadu posúdiť, či takéto opatrenia môžu byť primeraným riešením.
3. Pred spustením kamerového systému je prevádzkovateľ povinný posúdiť, kedy a kedy sú nevyhnutne potrebné opatrenia týkajúce sa videa. Monitorovací systém, ktorý pracuje v nočnej dobe, ako aj mimo riadneho pracovného času, bude zvyčajne spĺňať potreby prevádzkovateľa, aby sa predišlo nebezpečenstvám týkajúcim sa jeho majetku.
4. Pozri WP217, článok 29 Pracovná skupina, str. 24 seq. Pozri tiež prípad ECJ C-708/18 str.44

|  |  |
| --- | --- |
| Schválené | 10 |

1. Potreba použitia video monitorovania na ochranu priestorov prevádzkovateľa sa vo všeobecnosti končí na hranici pozemku.11 Existujú však prípady, kedy monitorovanie majetku nestačí na účinnú ochranu. V niektorých individuálnych prípadoch môže byť potrebné rozšíriť video monitorovanie aj do bezprostredného okolia priestorov. V tejto súvislosti by prevádzkovateľ mal zvážiť fyzické a technické prostriedky, napríklad blokovanie alebo pixelovanie nerelevantných oblastí.

Príklad: Kníhkupectvo chce chrániť svoje priestory pred vandalizmom. Vo všeobecnosti by kamery mali natáčať len samotné priestory, pretože na tento účel nie je potrebné monitorovať susedné priestory alebo verejné priestory v okolí kníhkupectva.

28.

1. Otázky týkajúce sa nevyhnutnosti spracovania tiež vyvstávajú v súvislosti so spôsobom uchovávania dôkazov. V niektorých prípadoch môže byť potrebné použiť riešenie vo forme čiernej skrinky, kde sa záznam automaticky odstráni po určitej dobe uchovania a prístup k nemu sa dosiahne iba v prípade nehody. V iných situáciách nemusí byť potrebné videozáznamy vôbec zaznamenávať, ale vhodnejšie je namiesto toho použiť monitorovanie v reálnom čase. Rozhodnutie medzi riešeniami čiernej skrinky a monitorovaním v reálnom čase by malo vychádzať aj z monitorovaného účelu. Ak je napríklad účelom video monitorovania uchovávanie dôkazov, metódy monitorovania v reálnom čase zvyčajne nie sú vhodné. Monitorovanie v reálnom čase môže byť niekedy aj intruzívnejšie ako ukladanie a automatické mazanie materiálu po obmedzenom časovom rámci (napr. ak niekto neustále sleduje monitor, môže to byť intruzívnejšie než v prípade, že ak takýto monitor vôbec neexistuje a materiál je priamo ukladaný do čiernej skrinky). V tejto súvislosti sa musí zohľadniť zásada minimalizácie údajov [článok 5 ods. 1 písm. c)]. Malo by sa tiež pamätať na to, že je možné, že prevádzkovateľ by mohol namiesto bezpečnostných videí použiť bezpečnostný personál, ktorý je schopný okamžite reagovať a zasiahnuť.

3.1.3 Vyvažovanie záujmov

1. Za predpokladu, že video monitorovanie je potrebné na ochranu oprávnených záujmov prevádzkovateľa, môže sa video monitorovanie uviesť do prevádzky len vtedy, ak oprávnené záujmy prevádzkovateľa alebo záujmy tretej strany (napr. Ochrana majetku alebo fyzická integrita) nie sú potlačené záujmami alebo základnými právami a slobodami dotknutej osoby. Prevádzkovateľ musí zvážiť 1) do akej miery má monitorovanie vplyv na záujmy, základné práva a slobody jednotlivcov a 2) či to má za následok porušenie alebo negatívne následky s ohľadom na práva dotknutej osoby. Vyvažovanie záujmov je v skutočnosti povinné. Základné práva a slobody na jednej strane a oprávnené záujmy prevádzkovateľa na druhej strane je potrebné dôkladne vyhodnotiť a vyvážiť.
2. V niektorých členských štátoch to môže tiež podliehať vnútroštátnym právnym predpisom.

|  |  |
| --- | --- |
| Schválené | 11 |

Príklad: Súkromná parkovacia spoločnosť si zdokumentovala opakované problémy s krádežami v zaparkovaných autách. Parkovacie miesto je otvorený priestor a je ľahko dostupné pre každého, je však zreteľne označené značkami a cestnými blokátormi obklopujúcimi priestor. Parkovacia spoločnosť má oprávnený záujem (predchádzať krádežiam v automobiloch zákazníkov) na monitorovanie oblasti počas dňa, keď sa stretávajú s problémami. Dotknuté osoby sú monitorované v obmedzenom časovom rámci, nie sú v oblasti na rekreačné účely a je tiež v ich vlastnom záujme, aby sa zabránilo krádeži. Záujem dotknutých osôb, ktoré sa nemajú monitorovať, je v tomto prípade potlačený oprávneným záujmom prevádzkovateľa.

Príklad: Reštaurácia sa rozhodne nainštalovať videokamery do toalety na kontrolu čistoty sociálnych zariadení. V tomto prípade právo dotknutých osôb jasne prevyšuje záujmy prevádzkovateľa, a preto tam kamery nemôžu byť nainštalované.

31.

*3.1.3.1 Rozhodovanie od prípadu k prípadu*

1. Keďže vyvažovanie prípadov je podľa nariadenia povinné, rozhodnutie sa musí prijať od prípadu k prípadu (pozri článok 6 ods. 1 písm. f)). Odkazovanie na abstraktné situácie alebo vzájomné porovnávanie podobných prípadov je nedostatočné. Prevádzkovateľ musí vyhodnotiť riziká narušenia práv dotknutej osoby; tu je rozhodujúcim kritériom intenzita zásahu do práv a slobôd jednotlivca.
2. Intenzita sa môže definovať, okrem iného, podľa druhu zhromažďovaných informácií (obsah informácií), rozsahu (hustota informácií, priestorový a geografický rozsah), počtu dotknutých osôb, buď ako konkrétne číslo alebo ako pomer k príslušnému počtu obyvateľov, príslušnej situácie, skutočných záujmov skupiny dotknutých osôb, alternatívnych prostriedkov, ako aj povahy a rozsahu vyhodnotenia údajov.
3. Dôležitými vyvažovacími faktormi môžu byť veľkosť oblasti, ktorá je monitorovaná, a množstvo monitorovaných dotknutých osôb. Použitie videa na vzdialenom území (napríklad na monitorovanie voľne žijúcich živočíchov alebo na ochranu kritickej infraštruktúry, napríklad súkromnej rádiovej anténe), sa musí posudzovať inak ako pri videu v pešej zóne alebo v nákupnom stredisku.

Príklad: Ak je nainštalovaná palubná kamera vozidla (napríklad na účely zhromažďovania dôkazov v prípade nehody), je dôležité zabezpečiť, aby táto kamera nepretržite nezaznamenávala premávku, ako aj osoby, ktoré sa nachádzajú blízko cesty. V opačnom prípade záujem o videozáznamy ako dôkaz v teoretickejšom prípade dopravnej nehody nemôže odôvodniť tento závažný zásah do práv dotknutých osôb.11

35.

*3.1.3.2* *Primerané očakávania dotknutých osôb*

1. Podľa Odôvodnenia č. 47 je potrebné starostlivo posúdiť existenciu oprávneného záujmu. Tu je potrebné zahrnúť odôvodnené očakávania dotknutej osoby v čase a v súvislosti so spracovaním jej osobných údajov. Pokiaľ ide o systematické monitorovanie, vzťah medzi subjektom údajov a prevádzkovateľom sa môže výrazne líšiť a môže ovplyvniť, aké odôvodnené očakávania by dotknutá osoba mohla mať. Výklad pojmu odôvodneného očakávania by sa nemal zakladať iba na predmetných subjektívnych očakávaniach. Rozhodujúcim kritériom musí byť skôr to, či objektívna tretia strana mohla odôvodnene očakávať a dospieť k záveru, že bude v tejto konkrétnej situácii podliehať monitorovaniu.

Schválené 12

1. Napríklad zamestnanec na svojom pracovisku vo väčšine prípadov pravdepodobne neočakáva, že bude monitorovaný svojim zamestnávateľom.12 Monitorovanie sa okrem toho neočakáva v ani súkromnej záhrade, v obytných zónach ani vo vyšetrovacích a liečebných miestnostiach. Rovnako nie je odôvodnené očakávať monitorovanie v sanitárnych alebo saunových zariadeniach - monitorovanie takýchto priestorov je intenzívnym vniknutím do práva vylúčených osôb. Oprávnené očakávania dotknutých osôb sú také, že v týchto oblastiach sa nebude konať žiadne video monitorovanie. Na druhej strane môže klient banky očakávať, že bude vo vnútri banky alebo prostredníctvom bankomatu monitorovaný.
2. Dotknuté osoby môžu tiež očakávať, že nebudú podliehať monitorovaniu vo verejne prístupných oblastiach, najmä ak sa tieto oblasti zvyčajne používajú na regeneráciu, oddych a trávenie voľného času, ako aj na miestach, kde sa jednotlivci zdržiavajú a/alebo komunikujú, ako sú napríklad zóny s lavičkami, stoly v reštauráciách, parky, kiná a fitnescentrum. Záujmy alebo práva a slobody dotknutej osoby tu často prevyšujú oprávnené záujmy prevádzkovateľa.

Príklad: Na toaletách dotknuté osoby očakávajú, že nebudú monitorované. Video monitorovanie napríklad na prevenciu nehôd nie je primerané.

39.

1. Označenia informujúce dotknutú osobu o videu monitorovaní nie sú relevantné pri určovaní toho, čo môže dotknutá osoba objektívne očakávať. To znamená, že napr. majiteľ obchodu sa nemôže spoľahnúť na to, že zákazníci majú objektívne očakávania, že budú monitorovaní len preto, že označenie pri vchode informuje o monitorovaní jednotlivcov.

3.2 Nevyhnutnosť plniť úlohu vykonávanú vo verejnom záujme alebo pri výkone verejnej moci zverenej kontrolórovi, Článok 6 (1) (e)

1. Podľa článku 6 ods. 1 písm. e) Osobné údaje by sa mohli spracovávať prostredníctvom video monitorovania, ak je potrebné vykonať úlohu vykonávanú vo verejnom záujme alebo pri výkone verejnej moci.13 Môže sa stať, že výkon úradnej moci neumožňuje takéto spracovanie, ale iné legislatívne základy, ako napríklad „zdravie a bezpečnosť“ na ochranu návštevníkov a zamestnancov, môžu poskytnúť obmedzený priestor na spracovanie, pričom sa stále zohľadnia povinnosti vyplývajúce z GDPR a práva dotknutých osôb.
2. Členské štáty môžu zachovať alebo zaviesť osobitné vnútroštátne právne predpisy týkajúce sa video monitorovania s cieľom prispôsobiť uplatňovanie pravidiel GDPR stanovením presnejších požiadaviek na spracovanie, pokiaľ je to v súlade so zásadami stanovenými v GDPR (napr. obmedzenie ukladania, proporcionalita).
3. Pozri tiež: Článok 29 Pracovná skupina, Stanovisko 2/2017 k spracovaniu údajov v práci, WP249, Schválené 8. júna 2017.
4. Základ pre spracúvanie ustanoví právo Únie alebo právo členského štátu »a« je nevyhnutný na vykonanie úlohy vykonávanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi (Článok 6 (3)).

|  |  |
| --- | --- |
| Schválené | 13 |

3.3 Súhlas, Článok 6 (1) (a)

1. Súhlas musí byť slobodný, konkrétny, informovaný a jednoznačný, ako je to uvedené v Usmerneniach k udeleniu súhlasu.14
2. Pokiaľ ide o systematické monitorovanie, súhlas dotknutej osoby môže vo výnimočných prípadoch slúžiť ako právny základ v súlade s článkom 7 (pozri Odôvodnenie 43). Je samozrejmé, že nástroje monitorovania sú technológiou, ktorá monitoruje neznámy počet ľudí naraz. Prevádzkovateľ sotva bude schopný dokázať, že dotknutá osoba dala súhlas pred spracovaním svojich osobných údajov (článok 7 ods. 1). Za predpokladu, že dotknutá osoba stiahne svoj súhlas, bude pre prevádzkovateľa ťažké dokázať, že osobné údaje sa už nespracúvajú (článok 7 ods. 3).

Príklad: Športovci môžu požadovať monitorovanie počas jednotlivých cvičení s cieľom analyzovať svoju techniku a výkon. Na druhej strane, ak športový klub prevezme iniciatívu na monitorovanie celého tímu na ten istý účel, udelený súhlas často nebude považovaný za platný, pretože jednotliví športovci sa môžu cítiť pod tlakom na udelenie súhlasu, aby ich odmietnutie súhlasu nepriaznivo neovplyvnilo spoluhráčov.

45.

1. Ak sa prevádzkovateľ chce spoliehať na súhlas, je jeho povinnosťou zabezpečiť, aby mu každá dotknutá osoba, ktorá vstúpi do oblasti a na ktorú sa vzťahuje monitorovanie, udelila svoj súhlas. Tento súhlas musí spĺňať podmienky článku 7. Vstup na vyznačené monitorované územie (napr. ľudia sú vyzvaní, aby prešli konkrétnou chodbou alebo bránou na vstup do monitorovaného priestoru), nepredstavuje vyhlásenie alebo jednoznačný kladné krok potrebný k udelenie súhlasu, pokiaľ nespĺňa kritériá uvedené v článkoch 4 a 7, ako sú opísané v Usmerneniach k udeleniu súhlasu.15
2. Vzhľadom na nerovnováhu právomocí medzi zamestnávateľmi a zamestnancami by sa zamestnávatelia vo väčšine prípadov nemali spoliehať na súhlas pri spracovaní osobných údajov, pretože je nepravdepodobné, že by boli poskytnuté slobodne. V tejto súvislosti by sa mali zohľadniť Usmernenia k udeleniu súhlasu.
3. Právne predpisy členského štátu alebo kolektívne zmluvy vrátane „pracovných zmlúv“ môžu ustanoviť osobitné pravidlá spracovania osobných údajov zamestnancov v kontexte zamestnania (pozri článok 88).
4. Článok 29 Pracovná skupina (Art. 29 WP) „Usmernenia k udeleniu súhlasu podľa nariadenia 2016/679“ (WP 259 rev. 01). - schválené EDPB
5. Článok 29 Pracovná skupina (Art. 29 WP) „Usmernenia k udeleniu súhlasu podľa nariadenia 2016/679“ (WP 259) - schválené EDPB – čo by sa malo zohľadniť.

|  |  |
| --- | --- |
| Schválené | 14 |

4 ZVEREJŇOVANIE VIDEOZÁZNAMOV TRETÍM STRANÁM

1. Na sprístupnenie videozáznamov tretím stranám sa v zásade vzťahuje všeobecné nariadenie GDPR.

4.1 Zverejňovanie videozáznamov tretím stranám vo všeobecnosti

1. Zverejnenie je definované v článku 4 ods. 2 ako prenos (napr. individuálna komunikácia), šírenie (napr. publikovanie online) alebo iné sprístupnenie. Tretie strany sú definované v článku 4 ods. 10. Ak sa informácie poskytujú tretím krajinám alebo medzinárodným organizáciám, osobitné ustanovenia článku 44 a nasl. sa tiež uplatňujú.
2. Akékoľvek zverejnenie osobných údajov je samostatným druhom spracovania osobných údajov, pre ktoré prevádzkovateľ potrebuje právny základ uvedený v článku 6.

Príklad: Prevádzkovateľ, ktorý chce nahrať záznam na internet, sa musí pri tomto spracovaní opierať o právny základ, napríklad získaním súhlasu dotknutej osoby podľa článku 6 ods. 1 písm. a).

52.

1. Prenos videozáznamov tretím stranám na iné účely, ako na ktoré boli zhromaždené, je možný podľa pravidiel uvedených v článku 6 ods. 4.

Príklad: Systém video monitorovania bariéry (na parkovisku) je nainštalovaný za účelom riešenia prípadných škôd. Vyskytne sa škoda a záznam je poskytnutý právnikovi, aby pokračoval v konaní. V takom prípade je účel nahrávania rovnaký ako účel prenosu.

Príklad: Systém video monitorovania bariéry (na parkovisku) je nainštalovaný za účelom riešenia prípadných škôd. Nahrávka je zverejnená online z čisto zábavných dôvodov. V takom prípade sa účel zmenil a nie je zlučiteľný s pôvodným účelom. Ďalej by bolo problematické určiť právny základ pre toto spracovanie (publikovanie).

54.

1. Príjemca tretej strany bude musieť vykonať vlastnú právnu analýzu, najmä určiť jeho právny základ podľa článku 6 na jeho spracovanie (napr. príjem materiálu).

4.2 Zverejnenie videozáznamov orgánom činným v trestnom konaní

1. Poskytovanie videozáznamov orgánom činným v trestnom konaní je tiež nezávislým procesom, ktorý si vyžaduje osobitné odôvodnenie pre prevádzkovateľa.
2. Podľa článku 6 ods. 1 písm. c) je spracovanie zákonné, ak je to potrebné na splnenie zákonnej povinnosti, ktorej podlieha prevádzkovateľ. Aj keď je uplatniteľné policajné právo záležitosťou, ktorá je pod výlučnou kontrolou členských štátov, s najväčšou pravdepodobnosťou existujú všeobecné pravidlá upravujúce odovzdávanie dôkazov orgánom činným v trestnom konaní v každom členskom štáte. Spracovanie odovzdávania údajov prevádzkovateľom je upravené v GDPR. Ak vnútroštátne právne predpisy vyžadujú, aby prevádzkovateľ spolupracoval s orgánmi činnými v trestnom konaní (napr. Vyšetrovanie), právnym základom pre odovzdanie údajov je zákonná povinnosť podľa článku 6 ods. 1 písm. c).
3. Obmedzenie účelu uvedené v článku 6 ods. 4 je potom často problematické, pretože zverejnenie sa výslovne týka práva členského štátu. Zohľadnenie osobitných požiadaviek na zmenu účelu v zmysle písmena a - e preto nie je potrebné.

|  |  |
| --- | --- |
| Schválené | 15 |

Príklad: Majiteľ obchodu vyhotovuje videozáznam pri vchode do obchodu. Zábery ukazujú, že niekto ukradol peňaženku inej osoby. Polícia žiada prevádzkovateľa, aby materiál odovzdal na pomoc pri vyšetrovaní. V takom prípade by vlastník obchodu použil právny základ podľa článku 6 ods. 1 písm. c) (právna povinnosť) v spojení s príslušným vnútroštátnym právom na spracovanie prevodu.

59.

Príklad: Kamera je nainštalovaná v obchode z bezpečnostných dôvodov. Majiteľ obchodu verí, že vo svojom zázname zaznamenal niečo podozrivé a rozhodol sa poslať materiál polícii (bez náznaku, že prebieha nejaké vyšetrovanie). V takom prípade musí majiteľ obchodu posúdiť, či sú vo väčšine prípadov splnené podmienky podľa článku 6 ods. 1 písm. F). Zvyčajne to tak je, ak majiteľ obchodu má dôvodné podozrenie, že bol spáchaný trestný čin.

60.

1. Spracovanie osobných údajov samotnými orgánmi činnými v trestnom konaní sa neriadi GDPR (pozri článok 2 ods. 2 písm. d)), ale namiesto toho sa riadi smernicou o presadzovaní práva (EU2016/680).

Schválené 16

5 SPRACÚVANIE OSOBITNÝCH KATEGÓRIÍ ÚDAJOV

1. Systémy video monitorovania zvyčajne zhromažďujú obrovské množstvá osobných údajov, ktoré môžu odhaliť údaje veľmi osobného charakteru, a dokonca aj osobitné kategórie údajov. V skutočnosti sa zjavne nepodstatné údaje pôvodne zhromaždené prostredníctvom videa môžu použiť na odvodenie iných informácií na dosiahnutie iného účelu (napr. na mapovanie zvykov jednotlivca). Video monitorovanie sa však vždy nepovažuje za spracovanie osobitných kategórií osobných údajov.

Príklad: Videozáznamy ukazujúce dotknutú osobu, ktorá nosí okuliare alebo používa invalidný vozík, sa samy osebe nepovažujú za osobitné kategórie osobných údajov.

63.

1. Ak sa však videozáznam spracováva s cieľom odvodiť osobitné kategórie údajov, uplatňuje sa článok 9.

Príklad: Politické stanoviská by mohli byť napríklad odvodené z obrázkov ukazujúcich identifikovateľné dotknuté osoby, ktoré sa zúčastňujú na udalosti, zúčastňujú sa štrajku atď. To by spadalo pod článok 9.

Príklad: Za spracovanie osobitných kategórií osobných údajov (článok 9) sa považuje aj nemocnica, ktorá inštaluje videokameru s cieľom monitorovať zdravotný stav pacienta.

65.

1. Vo všeobecnosti by sa zásadne mala pri inštalácii systému video monitorovania starostlivo zvážiť zásada minimalizácie údajov. Preto aj v prípadoch, keď sa článok 9 ods. 1 neuplatňuje, prevádzkovateľ údajov by sa mal vždy snažiť minimalizovať riziko zachytenia záznamu, ktorý odhalí iné citlivé údaje (nad rámec článku 9), bez ohľadu na cieľ.

Príklad: Video monitorovanie týkajúce sa kostola ako také nespadá do pôsobnosti článku 9. Prevádzkovateľ však musí vykonať mimoriadne starostlivé posúdenie podľa článku 6 ods. 1 písm. f), pričom musí zohľadniť povahu údajov, ako aj riziko zachytenia ďalších citlivých údajov (nad rámec článku 9) pri posudzovaní záujmov dotknutej osoby.

67.

1. Ak sa na spracovanie osobitných kategórií údajov používa systém videa, musí prevádzkovateľ údajov identifikovať tak výnimku pre spracovanie osobitných kategórií údajov podľa článku 9 (t. j. výnimka zo všeobecného pravidla, že by sa nemali spracúvať osobitné kategórie údajov) ako aj právny základ podľa článku 6.
2. Napríklad článok 9 ods. 2 písm. c) (“[…] *spracovanie je potrebné na ochranu životných záujmov dotknutej osoby alebo inej fyzickej osoby* […]”) by sa mohol - teoreticky a výnimočne - použiť, ale prevádzkovateľ údajov by to musel odôvodniť ako absolútnu nevyhnutnosť, ako chrániť základné záujmy osoby a preukázať, že „[…] dotknutá osoba je *fyzicky alebo právne neschopná udeliť svoj súhlas."*. Prevádzkovateľ údajov navyše nebude byť oprávnený používať systém z akéhokoľvek iného dôvodu.
3. V tejto súvislosti je dôležité poznamenať, že nie je pravdepodobné, že by každá výnimka uvedená v článku 9 bola použiteľná na odôvodnenie spracúvania osobitných kategórií údajov prostredníctvom video monitorovania. Konkrétnejšie, prevádzkovatelia údajov, ktorí spracúvajú tieto údaje v súvislosti s videom, sa nemôžu odvolávať na článok 9 ods. 2 písm. e), ktorý umožňuje spracovanie týkajúce sa osobných údajov, ktoré dotknutá osoba zjavne zverejňuje. Samotná skutočnosť, že sa osoba dostane do dosahu kamery, neznamená, že dotknutá osoba má v úmysle zverejniť osobitné kategórie údajov, ktoré sa jej týkajú.

|  |  |
| --- | --- |
| Schválené | 17 |

1. Navyše si spracúvanie osobitných kategórií údajov vyžaduje zvýšenú a nepretržitú ostražitosť voči niektorým povinnostiam; napríklad vysoká úroveň bezpečnosti a v prípade potreby aj hodnotenie bezpečnosti na ochranu údajov

Príklad: Zamestnávateľ nesmie používať video monitorovanie pre záznam demonštrácie s účelom identifikovať štrajkujúcich.

72.

5.1 Všeobecné úvahy pri spracovávaní biometrických údajov

1. Používanie biometrických údajov a najmä rozpoznávanie tváre so sebou prináša zvýšené riziká pre práva dotknutých osôb. Je nevyhnutné, aby sa tieto technológie využívali pri náležitom rešpektovaní zásad zákonnosti, nevyhnutnosti, proporcionality a minimalizácie údajov stanovených v GDPR. Zatiaľ čo používanie týchto technológií možno považovať za zvlášť účinné, prevádzkovatelia by mali predovšetkým posúdiť vplyv na základné práva a slobody a zvážiť menej rušivé prostriedky na dosiahnutie svojho legitímneho účelu spracovania.
2. Na to, aby sa spracovanie nespracovaných údajov, ako sú fyzikálne, fyziologické alebo behaviorálne charakteristiky fyzickej osoby, mohli považovať za biometrické údaje vymedzené v GDPR, musí zahŕňať meranie týchto charakteristík. Keďže biometrické údaje sú výsledkom takýchto meraní, GDPR vo svojom článku 4.14 uvádza, že “*[…]* *vyplýva zo špecifického technického spracovania týkajúceho sa fyzických, fyziologických alebo behaviorálnych charakteristík fyzickej osoby, ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby […]”.* Videozáznam jednotlivca sa však sám osebe nemôže považovať za biometrický údaj podľa článku 9, ak nebol špecificky technicky spracovaný s cieľom prispieť k identifikácii jednotlivca. 16
3. Aby sa mohlo považovať za spracovanie osobitných kategórií osobných údajov (článok 9), vyžaduje sa, aby sa biometrické údaje spracúvali „na účely jednoznačnej identifikácie fyzickej osoby“.
4. Pre zhrnutie sa vzhľadom na články 4.14 a 9 sa musia zvážiť tri kritériá:
	* **Povaha údajov:** údaje týkajúce sa fyzických, fyziologických alebo behaviorálnych charakteristík fyzickej osoby,
	* **Prostriedky a spôsob spracovania:** údaje „vyplývajúce zo špecifického technického spracovania“,
	* **Účel spracovania:** údaje sa musia používať na účely jednoznačnej identifikácie fyzickej osoby.
5. Využívanie video monitorovania vrátane funkcie biometrického rozpoznávania inštalovaného súkromnými subjektmi na vlastné účely (napr. marketing, štatistika alebo dokonca bezpečnosť) si vo väčšine prípadov vyžaduje výslovný súhlas všetkých dotknutých osôb (článok 9 ods. 2 písm. a)), avšak môže sa uplatniť aj iná vhodná výnimka z článku 9.

16 Odôvodnenie 51 GDPR podporuje túto analýzu a uvádza, že “*[…]* *Spracovanie fotografií by sa nemalo systematicky považovať za spracúvanie osobitných kategórií osobných údajov, keďže sa na ne vzťahuje definícia biometrických údajov iba v prípade, že sa spracúvajú osobitnými technickými prostriedkami umožňujúcimi jedinečnú identifikáciu alebo autentifikáciu fyzickej osoby. […]*”.

|  |  |
| --- | --- |
| Schválené | 18 |

Príklad: V záujme zlepšenia svojich služieb nahrádza súkromná spoločnosť miesta kontroly na identifikáciu cestujúcich na letisku (odloženie batožiny, nástup na palubu) systémami video monitorovania, ktoré používajú techniky rozpoznávania tváre na overenie totožnosti cestujúcich, ktorí sa rozhodli súhlasiť s takýmto postupom. Keďže spracovanie spadá pod článok 9, cestujúci, ktorí predtým dali svoj výslovný a informovaný súhlas, sa budú musieť prihlásiť napríklad do automatického terminálu, aby si mohli vytvoriť a zaregistrovať svoju šablónu tváre spojenú s ich palubným lístkom a totožnosťou. Kontrolné body s rozpoznávaním tváre musia byť jasne oddelené, napr. systém musí byť nainštalovaný v portáli, aby sa nezachytili biometrické šablóny nezúčastnenej osoby. Portál vybavený biometrickým systémom budú používať iba cestujúci, ktorí predtým dali svoj súhlas a pokračovali v registrácii.

Príklad: Prevádzkovateľ riadi prístup do svojej budovy pomocou metódy rozpoznania tváre. Ľudia môžu tento spôsob prístupu využívať iba vtedy, ak vopred poskytli výslovný informovaný súhlas (podľa článku 9 ods. 2 písm. a)). S cieľom zabezpečiť, aby nebol nikto, kto predtým nedal svoj súhlas, zachytený, metódu rozpoznania tváre by mala spustiť samotná dotknutá osoba, napríklad stlačením tlačidla. Na zabezpečenie zákonnosti spracovania musí prevádzkovateľ vždy ponúknuť alternatívny spôsob prístupu do budovy bez biometrického spracovania, ako sú odznaky alebo kľúče.

78.

1. V takomto type prípadov, keď sa generujú biometrické šablóny, prevádzkovatelia zabezpečia, aby po dosiahnutí výsledku zhody alebo nezhody boli všetky priebežné vyhotovené šablóny (s výslovným a informovaným súhlasom dotknutej osoby), ktoré mali za cieľ porovnanie s tými šablónami a ktoré vytvorili dotknuté osoby v čase zaradenia do systému, okamžite a bezpečne vymazané. Šablóny vytvorené pre zaradenie do systémy by sa mali uchovávať iba na účel účelu spracovania a nemali by sa uchovávať ani archivovať.
2. Ak však účelom spracovania je napríklad rozlíšiť jednu kategóriu ľudí od druhej, ale nie jednoznačne identifikovať niekoho, na takéto spracovanie sa nevzťahuje článok 9.

Príklad: Majiteľ obchodu by mal záujem prispôsobiť svoju reklamu na základe pohlavia a veku charakteristík zákazníka zachyteného systémom videa. Ak tento systém nevytvorí biometrické šablóny s cieľom jednoznačne identifikovať osoby, ale namiesto toho len zistí tieto fyzikálne vlastnosti s cieľom klasifikovať osobu, na takéto spracovanie by sa nevzťahoval článok 9 (pokiaľ sa nespracúvajú žiadne iné typy osobitných kategórií údajov).

81.

1. Článok 9 sa však uplatňuje, ak prevádzkovateľ ukladá biometrické údaje (najčastejšie prostredníctvom šablón, ktoré sa získavajú extrahovaním kľúčových prvkov zo surovej formy biometrických údajov (napr. meranie tváre z obrazu)) s cieľom jednoznačne identifikovať osobu. Ak chce prevádzkovateľ zistiť, či dotknutá osoba opäť vstúpila do oblasti alebo vstúpila do inej oblasti (napríklad s cieľom ponúkať nepretržite reklamu na mieru), potom by účelom bolo jednoznačne identifikovať fyzickú osobu, čo znamená, že operácia by od začiatku spadala do pôsobnosti článku 9. Taká situácia by mohla nastať, ak by prevádzkovateľ ukladal vytvorené šablóny na poskytovanie ďalšej reklamy prispôsobenej na niekoľko billboardov na rôznych miestach v obchode. Keďže systém využíva fyzikálne vlastnosti na detekciu konkrétnych jednotlivcov, ktorí sa vracajú do dosahu kamery (ako sú návštevníci nákupného centra) a ich monitorovanie, predstavuje to metódu biometrickej identifikácie, pretože jej cieľom je rozpoznávanie pomocou špecifického technického spracovania.

Schválené 19

Príklad: Majiteľ obchodu nainštaloval vo svojom obchode systém rozpoznávania tváre s cieľom prispôsobiť svoju reklamu jednotlivcom. Pred použitím tohto biometrického systému a doručením prispôsobenej reklamy musí prevádzkovateľ údajov získať výslovný a informovaný súhlas všetkých dotknutých osôb. Systém monitorovania by bol nezákonný, ak by zachytil návštevníkov alebo okoloidúcich, ktorí nesúhlasili s vytvorením ich biometrickej šablóny, aj keď sa ich šablóna v čo najkratšom čase vymaže. Tieto dočasné šablóny skutočne predstavujú biometrické údaje spracovávané s cieľom jednoznačne identifikovať osobu, ktorá nemusí mať záujem o cielenú reklamu.

83.

1. EDPB poznamenáva, že niektoré biometrické systémy sú nainštalované v nekontrolovaných prostrediach17, čo znamená, že tento systém zahŕňa priebežné zachytenie tvárí každého jednotlivca prechádzajúceho v dosahu kamery, vrátane osôb, ktoré nesúhlasili s biometrickým zariadením, a teda vytvorením biometrickej šablóny. Tieto šablóny sa porovnávajú so šablónami vytvorenými dotknutými osobami, ktoré dali svoj predchádzajúci súhlas počas procesu zaradenia do systému (t. j. užívateľ biometrického zariadenia), aby prevádzkovateľ údajov rozoznal, či daná osoba je používateľom biometrického zariadenia alebo nie. V tomto prípade je systém často navrhnutý tak, aby diskriminoval jednotlivcov, ktorých chce rozoznať z databázy od tých, ktorí v nej nie sú zaregistrovaní. Keďže účelom je jedinečná identifikácia fyzických osôb, pre kohokoľvek zachyteného kamerou je stále potrebná výnimka podľa článku 9 ods. 2 GDPR.

Príklad: Hotel používa video monitorovanie na automatické upozornenie manažéra hotela, že prišiel VIP hosť v momente, keď je rozpoznaná jeho tvár. Títo VIP hostia predtým, ako sú uložení v databáze zriadenej na tento účel, výslovne vyjadrili súhlas s používaním systému rozpoznávania tváre. Tieto systémy spracovania biometrických údajov by boli nezákonné, pokiaľ by všetci ostatní monitorovaní hostia (na účely identifikácie VIP) nesúhlasili so spracovaním podľa článku 9 ods. 2 písm. a) GDPR.

Príklad: Prevádzkovateľ inštaluje videozáznam s rozpoznaním tváre pri vstupe do koncertnej sály, ktorú spravuje. Prevádzkovateľ musí mať jasne oddelené vchody; jeden s biometrickým systémom a druhý bez (kde namiesto toho napríklad skenujete lístok). Vchody vybavené biometrickými zariadeniami musia byť nainštalované a sprístupnené takým spôsobom, ktorý zabráni systému v zachytávaní biometrických šablón nezúčastnených osôb.

85.

1. Nakoniec, ak sa vyžaduje súhlas podľa článku 9 GDPR, prevádzkovateľ údajov nepodmieňuje prístup k svojim službám akceptovaním biometrického spracovania. Inými slovami, a najmä ak sa biometrické spracovanie používa na účely autentifikácie, prevádzkovateľ údajov musí ponúknuť alternatívne riešenie, ktoré nezahŕňa biometrické spracovanie - bez obmedzení alebo dodatočných nákladov pre dotknutú osobu. Toto alternatívne riešenie je potrebné aj pre osoby, ktoré nespĺňajú obmedzenia biometrického zariadenia (registrácia alebo načítanie biometrických údajov je nemožné, situácia so zdravotným postihnutím sťažuje použitie atď.) a pri očakávaní nedostupnosti biometrického zariadenia (napr. porucha zariadenia), musí byť k dispozícii „záložné riešenie“, aby sa zabezpečila kontinuita navrhovanej služby, avšak obmedzená na výnimočné použitie. Vo výnimočných prípadoch môže nastať situácia, keď je spracovanie biometrických údajov hlavnou činnosťou služby poskytovanej na základe zmluvy, napr.

17 Znamená to, že biometrické zariadenie je umiestnené v priestore prístupnom verejnosti a je schopné pracovať s každým, kto okolo neho prechádza, na rozdiel od biometrických systémov v kontrolovanom prostredí, ktoré možno použiť len na základe súhlasu zúčastnenej osoby.

Schválené 20

múzeum, ktoré zriaďuje výstavu s cieľom demonštrovať použitie zariadenia na rozpoznávanie tváre. V takom prípade nebude môcť dotknutá osoba odmietnuť spracovanie biometrických údajov, ak sa chce na výstave zúčastniť. V takom prípade je súhlas požadovaný podľa článku 9 stále platný, ak sú splnené požiadavky článku 7.

5.2 Navrhované opatrenia na minimalizáciu rizík pri spracovaní biometrických údajov

1. V súlade so zásadou minimalizácie údajov musia prevádzkovatelia údajov zabezpečiť, aby údaje extrahované z digitálneho obrazu na zostavenie šablóny neboli nadmerné a aby obsahovali iba informácie požadované na určený účel, čím sa zabráni akémukoľvek možnému ďalšiemu spracovaniu. Mali by sa prijať opatrenia na zabezpečenie toho, aby sa šablóny nemohli preniesť cez biometrické systémy.
2. Identifikácia a autentifikácia/overenie si pravdepodobne budú vyžadovať uloženie šablóny na použitie pre neskoršie porovnanie. Prevádzkovateľ údajov musí zvážiť najvhodnejšie miesto na uloženie údajov. V prostredí pod kontrolou (ohraničené chodby alebo miesta kontroly) sa šablóny ukladajú na jednotlivých zariadeniach uchovávaných používateľom a pod jeho výlučnou kontrolou (v smartfóne alebo na identifikačnej karte) alebo - ak je to potrebné na konkrétne účely a v prítomnosti objektívnych potrieb - uložené v centralizovanej databáze v zašifrovanej podobe pod kľúčom/heslom výlučne v rukách danej osoby, aby sa zabránilo neoprávnenému prístupu k šablóne alebo úložisku. Ak sa prevádzkovateľ údajov nemôže vyhnúť prístupu k šablónam, musí podniknúť príslušné kroky na zabezpečenie bezpečnosti uložených údajov. To môže zahŕňať šifrovanie šablóny pomocou kryptografického algoritmu.
3. V každom prípade prevádzkovateľ prijme všetky potrebné opatrenia na zachovanie dostupnosti, integrity a dôvernosti spracovávaných údajov. Na tento účel prevádzkovateľ prijme najmä tieto opatrenia: rozdelí údaje počas prenosu a ukladania, uloží biometrické šablóny a nespracované údaje alebo údaje o totožnosti do rôznych databáz, zašifruje biometrické údaje, najmä biometrické šablóny, a vymedzí politiku šifrovania a zaheslovania, bude integrovať organizačné a technické opatrenie na zisťovanie podvodov, priradí k údajom kód integrity (napríklad podpis alebo digitálny odtlačok hash) a zakáže akýkoľvek externý prístup k biometrickým údajom. Takéto opatrenia sa budú musieť vyvíjať spolu s pokrokom v technológiách.
4. Prevádzkovatelia údajov by okrem toho mali pristúpiť k vymazaniu prvotných nespracovaných údajov (záznamy tváre, rečové signály, chôdza atď.) a zabezpečiť účinnosť tohto vymazania. Ak už neexistuje právny základ na spracovanie, nespracované údaje sa musia vymazať. Pokiaľ biometrické šablóny pochádzajú z takýchto údajov, je skutočne možné usúdiť, že zostavenie databáz by mohlo predstavovať rovnaké, ak nie dokonca väčšie ohrozenie (pretože biometrická šablóna nemusí byť vždy ľahko čitateľná bez znalosti toho, ako bola naprogramovaná, zatiaľ čo nespracované údaje budú základnými kameňmi každej šablóny). V prípade, že by prevádzkovateľ údajov potreboval takéto údaje uchovať, je potrebné preskúmať metódy šumu (napríklad vodotlač), ktoré by spôsobili neefektívnosť vytvorenia šablóny. Prevádzkovateľ musí tiež odstrániť biometrické údaje a šablóny v prípade neoprávneného prístupu k terminálu na porovnávanie načítaných údajov alebo k úložnému serveru a vymazať všetky údaje, ktoré nie sú užitočné na ďalšie spracovanie na konci životnosti biometrického zariadenia.

Schválené 21

6 PRÁVA DOTKNUTEJ OSOBY

1. Kvôli charakteru spracovania údajov pri použití videa spadajú práva niektorých dotknutých osôb podľa GDPR ďalšiemu objasneniu. Táto kapitola však nie je vyčerpávajúca, všetky práva v rámci GDPR sa vzťahujú na spracovanie osobných údajov prostredníctvom video monitorovania.

6.1 Právo na prístup

1. Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa jej osobné údaje spracúvajú alebo nie. Pokiaľ ide o video monitorovanie, znamená to, že ak sa žiadne údaje neukladajú ani žiadnym spôsobom neprenášajú, prevádzkovateľ môže po uplynutí momentu monitorovania v reálnom čase poskytnúť iba informáciu, že žiadne osobné údaje sa už nespracúvajú (okrem všeobecných povinností týkajúcich sa informácií podľa článku 13, *pozri oddiel 7* *–* *Povinnosti týkajúce sa transparentnosti a informovania*). Ak sa však údaje stále spracovávajú v čase žiadosti (t. j. ak sa údaje ukladajú alebo nepretržite spracovávajú iným spôsobom), dotknutá osoba by mala dostať prístup a informácie v súlade s článkom 15.
2. Existuje však niekoľko obmedzení, ktoré sa môžu v niektorých prípadoch vzťahovať na právo na prístup.
	* Článok 15 ods. 4 GDPR, nepriaznivo ovplyvňuje práva ostatných
3. Vzhľadom na to, že v rovnakej sekvencii video monitorovania môže byť zaznamenaný ľubovoľný počet dotknutých osôb, skríning (detekčná kontrola) by potom spôsobil ďalšie spracovanie osobných údajov iných dotknutých osôb. Ak chce dotknutá osoba získať kópiu materiálu (článok 15 ods. 3), mohlo by to nepriaznivo ovplyvniť práva a slobody ostatných dotknutých osôb v materiáli. Aby sa tomu zabránilo, prevádzkovateľ by preto mal vziať do úvahy, že z dôvodu intruzívneho charakteru video monitorovania by prevádzkovateľ nemal v niektorých prípadoch odovzdávať videozáznamy, kde je možné identifikovať iných aktérov. Ochrana práv tretích strán by sa však nemala využívať ako ospravedlnenie na zabránenie oprávneným nárokom na prístup jednotlivcov. Prevádzkovateľ by mal v týchto prípadoch implementovať technické opatrenia na splnenie žiadosti o prístup (napríklad úpravou obrázkov, ako je napríklad vyšrafovanie alebo zakódovanie). Prevádzkovatelia však nie sú povinní implementovať takéto technické opatrenia, ak dokážu žiadosti podľa článku 15 zabezpečiť inak a v lehote stanovenej v článku 12 ods. 3.
	* Článok 11 ods. 2 GDPR, prevádzkovateľ nie je schopný identifikovať dotknutú osobu
4. Ak sa vo videozázname nedajú vyhľadávať osobné údaje (t. j. prevádzkovateľ by pravdepodobne musel prejsť veľkým množstvom uloženého materiálu, aby mohol nájsť dotknutú osobu), prevádzkovateľ nemusí byť schopný dotknutú osobu identifikovať.
5. Z týchto dôvodov musí dotknutá osoba (okrem toho, že sa identifikuje identifikačným dokladom alebo osobne), vo svojej žiadosti adresovanej prevádzkovateľovi uviesť, kedy - v primeranom časovom rámci úmerne k počtu zaznamenaných osôb - vstúpila do monitorovanej oblasti , Prevádzkovateľ by mal vopred informovať dotknutú osobu o tom, aké informácie je potrebné poskytnúť, aby prevádzkovateľ mohol vyhovieť žiadosti. Ak je prevádzkovateľ schopný preukázať, že nie je schopný identifikovať dotknutú osobu, musí o tom podľa možností dotknutú osobu informovať. V takejto situácii by mal prevádzkovateľ v reakcii na žiadosť dotknutej osoby ju informovať o presnej oblasti monitorovania, overovanie používaných kamier atď., aby dotknutá osoba mohla úplne pochopiť, aké osobné údaje o nej mohli byť spracované.

|  |  |
| --- | --- |
| Schválené | 22 |

Príklad: Ak dotknutá osoba požiada o kópiu svojich osobných údajov spracúvaných prostredníctvom video monitorovania pri vstupe do nákupného centra s 30 000 návštevami za deň, dotknutá osoba by mala uviesť, kedy prešla monitorovanou oblasťou približne v rámci časového rámca jednej hodiny. Ak prevádzkovateľ materiál stále spracúva, mala by sa dotknutej osobe poskytnúť kópia videozáznamu. Ak možno v tom istom materiáli identifikovať ďalšie dotknuté osoby, mala by sa táto časť materiálu anonymizovať (napríklad rozmazaním kópie alebo jej častí) pred tým, ako sa daná kópia zašle dotknutej osobe, ktorá podala žiadosť.

Príklad: Ak prevádzkovateľ automaticky vymaže všetky zábery napríklad do 2 dní, prevádzkovateľ po týchto 2 dňoch nemôže poskytnúť záznam dotknutej osobe. Ak prevádzkovateľ dostane žiadosť po týchto dvoch dňoch, dotknutá osoba by o tom mala byť informovaná.

97.

* + Článok 12 GDPR, nadmerné požiadavky
1. V prípade neprimeraných alebo zjavne neopodstatnených žiadostí dotknutej osoby si môže prevádzkovateľ účtovať primeraný poplatok v súlade s článkom 12 ods. 5 písm. a) GDPR, alebo môže odmietnuť vyhovieť žiadosti (článok 12 ods. 5 písm. b) GDPR). Prevádzkovateľ musí byť schopný preukázať zjavne neopodstatnenú alebo neprimeranú povahu žiadosti.

6.2 Právo na výmaz a právo namietať

6.2.1 Právo na vymazanie (Právo byť zabudnutý)

1. Ak prevádzkovateľ naďalej spracúva osobné údaje nad rámec monitorovania v reálnom čase (napr. uchovávanie), dotknutá osoba môže požiadať o vymazanie osobných údajov podľa článku 17 GDPR.
2. Na žiadosť je prevádzkovateľ povinný osobné údaje bez zbytočného odkladu vymazať, ak sa uplatňuje jedna z okolností uvedených v článku 17 ods. 1 GDPR (a neuplatňuje sa žiadna z výnimiek uvedených v článku 17 ods. 3 GDPR). Zahŕňa to povinnosť vymazať osobné údaje, ak už nie sú potrebné na účel, na ktorý boli pôvodne uložené, alebo ak je spracovanie nezákonné. (pozri tiež *Oddiel 8 – Obdobia uchovávania a povinnosť vymazania*). Okrem toho by sa v závislosti od právneho základu spracovania mali osobné údaje vymazať:
	* pri súhlase, ak sa daný súhlas stiahne (a neexistuje žiadny iný právny základ na spracovanie) a
	* pri oprávnenom záujme:
3. vždy, keď dotknutá osoba uplatňuje právo namietať (pozri oddiel 6.2.2) a neexistujú závažné naliehavé oprávnené dôvody na spracovanie, alebo
	1. v prípade priameho marketingu (vrátane profilovania) vždy, keď dotknutá osoba namieta proti spracovaniu.
4. Ak prevádzkovateľ zverejnil videozáznam (napr. cez TV vysielanie alebo online vysielanie), je potrebné prijať primerané opatrenia s cieľom informovať ostatných prevádzkovateľov (ktorí v súčasnosti spracúvajú príslušné osobné údaje) o žiadosti podľa článku 17 ods. 2. GDPR. Primerané kroky by mali zahŕňať technické opatrenia, berúc do úvahy dostupnú technológiu a náklady na implementáciu. Prevádzkovateľ by mal podľa možnosti v súlade s článkom 19 GDPR informovať o vymazaní osobných údajov každého účastníka, ktorému boli osobné údaje predtým poskytnuté.

Schválené 23

1. Okrem povinnosti prevádzkovateľa vymazať osobné údaje na žiadosť dotknutej osoby je prevádzkovateľ povinný podľa všeobecných zásad GDPR obmedziť uložené osobné údaje (pozri oddiel 8).
2. Pre video monitorovanie je potrebné poznamenať, že napríklad rozmazaním obrazu bez spätnej schopnosti obnoviť osobné údaje, ktoré obraz predtým obsahoval, sa osobné údaje považujú za vymazané v súlade s GDPR..

Príklad: Obchod so zmiešaným tovarom má problémy s vandalizmom najmä na svojej vonkajšej strane, a preto využíva videozáznam mimo svojho vchodu v priamom spojení so stenami. Okoloidúci požiada obchod, aby od momentu používania video monitorovania vymazal jeho osobné údaje. Prevádzkovateľ je povinný odpovedať na žiadosť bez zbytočného odkladu a najneskôr do jedného mesiaca. Keďže predmetný záznam už nespĺňa účel, na ktorý bol pôvodne uložený (v čase, keď prechádzala dotknutá osoba okolo, nedošlo k vandalizmu), v čase žiadosti neexistuje žiadny oprávnený záujem na uložení údajov, ktoré by prevyšovali záujmy dotknutých osôb. Prevádzkovateľ musí osobné údaje vymazať.

104.

6.2.2 Právo namietať

1. Pokiaľ ide o video monitorovanie založené na oprávnenom záujme (článok 6 ods. 1 písm. f) GDPR) alebo na nevyhnutnosť pri vykonávaní úlohy vo verejnom záujme [článok 6 ods. 1 písm. e) GDPR], má dotknutá osoba právo - kedykoľvek - vzniesť námietky proti spracovaniu v súlade s článkom 21 GDPR z dôvodov týkajúcich sa jeho konkrétnej situácie. Pokiaľ prevádzkovateľ nepreukáže presvedčivé oprávnené dôvody, ktoré prevažujú nad právami a záujmami dotknutej osoby, musí sa spracovanie údajov jednotlivca, ktorý vzniesol námietku, zastaviť. Prevádzkovateľ by mal byť povinný odpovedať na žiadosti dotknutej osoby bez zbytočného odkladu a najneskôr do jedného mesiaca.
2. V súvislosti s videom monitorovaním môže byť táto námietka vznesená buď pri vstupe, v čase alebo po opustení monitorovanej oblasti. V praxi to znamená, že pokiaľ prevádzkovateľ nemá presvedčivé legitímne dôvody, monitorovanie oblasti, v ktorej by bolo možné identifikovať fyzické osoby, je zákonné iba vtedy,
	* 1. ak je prevádzkovateľ schopný okamžite zastaviť kameru pri spracovaní osobných údajov, ak o je o to požiadaný, alebo
		2. ak monitorovaná oblasť je tak podrobne vymedzená, že si prevádzkovateľ dokáže zabezpečiť súhlas dotknutej osoby pred vstupom do danej oblasti a nie je to oblasť, do ktorej má dotknutá osoba na prístup ako občan právo.
3. Cieľom týchto usmernení nie je zistiť, čo sa považuje za presvedčivý oprávnený záujem (článok 21 GDPR).
4. Pri použití video monitorovanie na účely priameho marketingu má dotknutá osoba právo namietať spracovanie na základe svojho uváženia, pretože právo namietať je v tomto kontexte absolútne (článok 21 ods. 2 a 3 GDPR).

|  |  |
| --- | --- |
| Schválené | 24 |

Príklad: Spoločnosť má ťažkosti s narušovaním bezpečnosti pri svojom vchode a používa video na základe oprávneného záujmu s cieľom chytiť tých, ktorí vstupujú do budovy neoprávnene. Návštevník má námietky proti spracovaniu svojich údajov prostredníctvom systému video monitorovania z dôvodov týkajúcich sa jeho konkrétnej situácie. Spoločnosť však v tomto prípade jeho žiadosť odmieta s vysvetlením, že uložené záznamy sú potrebné z dôvodu prebiehajúceho interného vyšetrovania, a preto majú presvedčivé oprávnené dôvody na ďalšie spracovanie osobných údajov.

109.

Schválené 25

7 POVINNOSTI TÝKAJÚCE SA TRANSPARENTNOSTI A INFORMOVANIA18

1. V európskych právnych predpisoch o ochrane údajov je už dlho zakomponované, že dotknuté osoby by si mali byť vedomé skutočnosti, že video monitorovanie je na danom mieste v prevádzke. Mali by byť podrobne informované o monitorovaných miestach.19 V rámci GDPR sú všeobecné Povinnosti týkajúce sa transparentnosti a informovania stanovené v článku 12 GDPR a nasledujúce. Ďalšie pokyny sú uvedené v Pracovnou skupinou vypracovaných „Usmerneniach pre transparentnosť podľa nariadenia 2016/679 (WP260)“, ktoré EDPB schválila 25. mája 2018. V súlade s WP260 ods. 26, je to článok 13 GDPR, ktorý sa uplatňuje, ak sa osobné údaje „[…] dotknutej osoby zbierajú pozorovaním (napr. pomocou automatických zariadení na zaznamenávanie údajov alebo softvéru na zaznamenávanie údajov, ako sú kamery […]“).
2. Na základe objemu informácií, ktoré sa majú poskytnúť dotknutej osobe, môžu prevádzkovatelia postupovať podľa vrstvených prístupov, kde sa rozhodnú používať kombináciu metód na zabezpečenie transparentnosti (WP260, odsek 35; WP89, odsek 22). Pokiaľ ide o video monitorovanie, najdôležitejšie informácie by sa mali zobraziť na samotnom výstražnom označení (prvá vrstva), zatiaľ čo ďalšie povinné údaje sa môžu poskytnúť inými prostriedkami (druhá vrstva).

7.1 Informácie prvej vrstvy (výstražné označenie)

1. Prvá vrstva sa týka primárneho spôsobu, akým sa prevádzkovateľ prvýkrát dostáva do kontaktu s dotknutou osobou. V tejto fáze môžu prevádzkovatelia použiť výstražné označenie, ktoré poukazuje na príslušné informácie. Zobrazené informácie sa môžu poskytovať v kombinácii s ikonou, aby poskytli ľahko viditeľným, zrozumiteľným a jasne čitateľným spôsobom zmysluplný prehľad o zamýšľanom spracovaní (článok 12 ods. 7 GDPR). Formát informovania by mal byť prispôsobený jednotlivým miestam (WP89 odsek 22).

7.1.1 Umiestnenie výstražného označenia

1. Informácie by mali byť umiestnené tak, aby dotknutá osoba mohla ľahko rozpoznať okolnosti monitorovania ešte pred vstupom do monitorovanej oblasti (približne na úrovni očí). Nie je potrebné odhaľovať polohu kamery, pokiaľ neexistujú pochybnosti o tom, ktoré oblasti sú predmetom monitorovania, a kontext monitorovania je jednoznačne objasnený (WP 89, odsek 22). Dotknutá osoba musí byť schopná odhadnúť, ktorá oblasť je zachytená kamerou, aby sa mohla vyhnúť monitorovaniu alebo v prípade potreby prispôsobila tomu svoje správanie.

7.1.2 Obsah prvej vrstvy

1. Informácie prvej vrstvy (výstražné označenie) by mali vo všeobecnosti poskytovať najdôležitejšie informácie, napr. podrobnosti o účeloch spracovania, totožnosti prevádzkovateľa a existencii práv dotknutej osoby, spolu s informáciami o najväčších dopadoch spracovania.20 To môže zahŕňať napríklad oprávnené záujmy, ktoré sleduje prevádzkovateľ (alebo tretia strana), a kontaktné údaje zodpovednej osoby (ak je to aplikovateľné). Musí tiež odkazovať na podrobnejšiu druhú vrstvu informácií a kde a ako ich nájsť.
2. Okrem toho by označenie malo obsahovať aj všetky informácie, ktoré by mohli dotknutú osobu prekvapiť (WP260, odsek 38). Mohli by to byť napríklad prenosy tretím stranám, najmä ak sa

18 Môžu sa uplatniť osobitné požiadavky vnútroštátnych právnych predpisov.

19 Pozri WP859, Stanovisko 4/2004 k spracovaniu osobných údajov prostredníctvom videozáznam, Článok 29 Pracovná skupina).

20 Pozri WP260, odsek 38.

Schválené 26

nachádzajú mimo EÚ, a doba uchovávania. Ak táto informácia nie je uvedená, dotknutá osoba by mala mať možnosť veriť, že existuje iba živé monitorovanie (bez zaznamenávania údajov alebo prenosu tretím stranám).



Príklad (nezáväzný návrh):

**Totožnosť prevádzkovateľa a prípadne zástupcu prevádzkovateľa:**

**Kontaktné údaje vrátane prípadnej zodpovednej osoby:**

**Informácie o spracovaní, ktoré má najväčší vplyv na dotknutú osobu (napr. retenčné obdobie alebo živé monitorovanie, zverejňovanie alebo prenos videozáznamov tretím stranám):**

**Účely video monitorovanie:**

 **Video monitorovanie!**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| K dispozícii sú ďalšie informácie: |  |  |  |  |
| prostredníctvom oznámenia |  | **Práva dotknutej osoby:** Ako dotknutá osoba máte niekoľko práv, najmä právo požadovať |  |
| na našej recepcii/v centre zákazníkom / |  |  |  |  |
|  | od prevádzkovateľa prístup k vašim osobným údajom alebo ich vymazanie.. |  |
|  v registri |  |  |
|  |  |  |  |
| cez internet (URL)… |  | Podrobné informácie o tomto videu vrátane vašich práv nájdete v úplných informáciách poskytnutých prevádzkovateľom prostredníctvom možností uvedených vľavo. |  |
|  |  |  |
|  |  |  |
|  |  |  |  |  |

116.

7.2 Informácie druhej vrstvy

1. Informácie druhej vrstvy musia byť k dispozícii na mieste ľahko prístupnom dotknutej osobe, napríklad ako úplný informačný hárok dostupný v centrálnom mieste (napr. informačný pult, recepcia alebo pokladňa) alebo vystavený na ľahko prístupnom plagáte. Ako je uvedené vyššie, výstražné označenie prvej vrstvy musí jasne odkazovať na informácie o vrstvách. Ďalej je najlepšie, ak sa informácie prvej vrstvy týkajú digitálneho zdroja (napríklad QR kódu alebo adresy webových stránok) druhej vrstvy. Informácie by však mali byť ľahko dostupné aj digitálne. Prístup k informáciám by malo byť možné bez vstupu do skúmanej oblasti, najmä ak sa informácie poskytujú digitálne (to sa dá dosiahnuť napríklad odkazom). Ďalším vhodným prostriedkom by mohlo byť telefónne číslo, na ktoré je možné zavolať. Poskytnuté informácie však musia obsahovať všetko, čo je povinnosťou podľa článku 13 GDPR.
2. EDPB okrem týchto možností a tiež na ich zefektívnenie podporuje využívanie technologických prostriedkov na poskytovanie informácií dotknutým osobám. To môže zahŕňať napríklad geografické lokalizačné kamery a zahrnutie informácií do mapovacích aplikácií alebo webových stránok, aby jednotlivci mohli na jednej strane ľahko identifikovať a špecifikovať zdroje videa súvisiace s výkonom svojich práv, a na druhej strane získať podrobnejšie informácie o spracovaní operácie.

Príklad: Majiteľ obchodu monitoruje svoj obchod. Na dosiahnutie súladu s článkom 13 stačí umiestniť výstražné označenie na ľahko viditeľné miesto pri vchode do jeho obchodu, ktorý obsahuje informácie o prvej vrstve. Okrem toho musí poskytnúť informačný list obsahujúci informácie o vrstvách v pokladni alebo na inom centrálnom a ľahko prístupnom mieste vo svojom obchode.

119.

Schválené 27

8 OBDOBIA UCHOVÁVANIA A POVINNOSŤ VYMAZANIA

1. Osobné údaje sa nemôžu uchovávať dlhšie, ako je potrebné na účely, na ktoré sa osobné údaje spracúvajú [článok 5 ods. 1 písm. C) a e) GDPR]. V niektorých členských štátoch môžu existovať osobitné ustanovenia týkajúce sa období uchovávania, pokiaľ ide o videozáznamy v súlade s článkom 6 ods. 2 GDPR.
2. To, či je potrebné osobné údaje uchovať alebo nie, by sa malo kontrolovať v úzkom časovom rámci. Vo všeobecnosti sú legitímnymi účelmi videozáznamu často ochrana majetku alebo pre uchovávanie dôkazov. Zvyčajne platí, že vzniknuté škody môžu byť uznané do jedného alebo dvoch dní. Na uľahčenie preukázania súladu s rámcom ochrany údajov je v záujme prevádzkovateľa vopred pripraviť organizačné opatrenia (napr. v prípade potreby vymenovať zástupcu na kontrolu a zabezpečenie videozáznamu). Pri zohľadnení zásad článku 5 ods. 1 písm. c) a e) GDPR, konkrétne minimalizácia údajov a obmedzenie uchovávania údajov, by sa osobné údaje mali vo väčšine prípadov (napr. na účely odhalenia vandalizmu) vymazať, najlepšie automaticky po niekoľkých dňoch. Čím dlhšie je stanovené obdobie uchovávania (najmä ak presahuje 72 hodín), tým viac musí byť predložená argumentácia o legitimite účelu a nevyhnutnosti uchovávania. Ak prevádzkovateľ používa videozáznamy nielen na monitorovanie svojich priestorov, ale tiež má v úmysle údaje uchovávať, musí zabezpečiť, aby bolo úložisko skutočne potrebné na dosiahnutie tohto účelu. Ak je to tak, obdobie uchovania musí byť jasne definované a individuálne stanovené pre každý konkrétny účel. Prevádzkovateľ je zodpovedný za vymedzenie doby uchovávania v súlade so zásadami nevyhnutnosti a proporcionality a za preukázanie súladu s ustanoveniami nariadenia o rozpočtových pravidlách.

Príklad: Majiteľ malej predajne by pravdepodobne nahlásil vandalizmus ešte v ten istý deň, ako sa stal. V dôsledku toho postačuje obvyklé obdobie uchovania 24 hodín. Ak má však cez víkendy zatvorené alebo sú dlhšie sviatky, môže to byť dôvodom na dlhšiu dobu uchovania. Ak sa zistí poškodenie, môže tiež potrebovať uložiť videozáznam dlhšiu dobu, aby mohol podniknúť právne kroky proti páchateľovi.

122.

9 TECHNICKÉ A ORGANIZAČNÉ OPATRENIA

1. Ako sa uvádza v článku 32 ods. 1 GDPR, spracovanie osobných údajov počas video monitorovania musí byť nielen zákonné prípustné, ale prevádzkovatelia a sprostredkovatelia ich musia tiež primerane zabezpečiť. **Implementované organizačné a technické opatrenia musia byť primerané rizikám vyplývajúcim z práv a slobôd fyzických osôb**, ktoré vyplývajú z náhodného alebo nezákonného zničenia, straty, zmeny, neoprávneného zverejnenia alebo prístupu k údajom z videozáznamov. Podľa článkov 24 a 25 GDPR musia prevádzkovatelia vykonávať technické a organizačné opatrenia aj s cieľom zabezpečiť počas spracovania všetky zásady ochrany údajov a vytvoriť prostriedky na vykonávanie práv dotknutých osôb uvedených v článkoch 15 - 22 GDPR. Prevádzkovatelia údajov by mali prijať interný rámec a politiky, ktorými sa zabezpečí toto vykonávanie tak v čase stanovenia prostriedkov na spracovanie, ako aj v čase samotného spracovania, vrátane vykonávania hodnotení vplyvu na ochranu údajov.

|  |  |
| --- | --- |
| Schválené | 28 |

9.1 Prehľad systému video monitorovania

1. Systém video monitorovania (VSS)21 pozostáva z analógových a digitálnych zariadení, ako aj softvéru na účely snímania obrazov scény, manipulácie s nimi a ich zobrazovania jeho prevádzkovateľovi. Jeho komponenty sú rozdelené do nasledujúcich kategórií:
* Video prostredie: snímanie obrazu, prepojenia a manipulácia s obrazom:
1. účelom snímania obrazu je generovanie obrazu skutočného sveta v takom formáte, že ho môže použiť zvyšok systému,
2. prepojenia opisujú všetok prenos údajov vo video prostredí, t. j. spojenia a komunikácie. Príkladmi pripojení sú káble, digitálne siete a bezdrôtové prenosy. Komunikácia popisuje všetky obrazové a kontrolné dátové signály, ktoré môžu byť digitálne alebo analógové,
	1. manipulácia s obrazom zahŕňa analýzu, uloženie a prezentáciu obrázka alebo postupnosti obrazov.
* Z pohľadu riadenia systému má VSS nasledujúce logické funkcie:
	1. správa údajov a riadenie činností, ktoré zahŕňa spracovanie príkazov prevádzkovateľa a činnosti generované systémom (výstražné postupy, varovanie prevádzkovateľa),
	2. rozhrania s inými systémami môžu zahŕňať pripojenie k iným bezpečnostným systémom (kontrola prístupu, požiarny poplach) a iným ako zabezpečovacím systémom (systémy riadenia budov, automatické rozpoznávanie poznávacích značiek).
* Bezpečnosť VSS spočíva v dôvernosti, integrite a dostupnosti systému a údajov:
	1. zabezpečenie systému zahŕňa fyzické zabezpečenie všetkých komponentov systému a kontrolu prístupu k VSS,
1. bezpečnosť údajov zahŕňa predchádzanie strate alebo manipulácii s údajmi.
2. GDPR neposkytuje definíciu, technický popis je napríklad uvedený v EN 62676-1-1: 2014 Systémy video videí na použitie v bezpečnostných aplikáciách - Časť 1-1: Požiadavky na videosystémy.

|  |  |
| --- | --- |
| Schválené | 29 |



125.

*Obrázok 1- Systém video monitorovania*

9.2 Ochrana údajov podľa návrhu a podľa štandardu

1. Ako sa uvádza v článku 25 GDPR, prevádzkovatelia musia implementovať primeranú ochranu údajov, hneď ako plánujú vykonávať video monitorovanie - pred začatím zhromažďovania a spracovania videozáznamov. Tieto zásady zdôrazňujú potrebu zabudovaných technológií zvyšujúcich súkromie, predvolených nastavení, ktoré minimalizujú spracovanie údajov, a poskytnutia potrebných nástrojov, ktoré umožňujú najvyššiu možnú ochranu osobných údajov.22.
2. Prevádzkovatelia by mali zabudovať záruky ochrany údajov a súkromia nielen do projektových špecifikácií technológie, ale aj do organizačných postupov. Pokiaľ ide o organizačné praktiky, prevádzkovateľ by mal prijať vhodný riadiaci rámec, ustanoviť a presadzovať politiky a postupy týkajúce sa video monitorovania. Z technického hľadiska by špecifikácia a návrh systému mali zahŕňať požiadavky na spracovanie osobných údajov v súlade so zásadami stanovenými v článku 5 GDPR (zákonnosť spracovania, účel a obmedzenie údajov, minimalizácia údajov v predvolenom nastavení v zmysle článku 25 ods. 2 GDPR , integrita a dôvernosť, zodpovednosť atď.). V prípade, že prevádzkovateľ plánuje získať systém video monitorovania na komerčné účely, musí zahrnúť tieto požiadavky do špecifikácie nákupu. Prevádzkovateľ musí zabezpečiť súlad s týmito požiadavkami, ktoré sa vzťahujú na všetky komponenty systému a na všetky údaje, ktoré spracováva, počas ich celého životného cyklu.

9.3 Konkrétne príklady príslušných opatrení

1. Väčšina opatrení, ktoré sa dajú použiť na zabezpečenie video monitorovania, sa nebude líšiť od opatrení používaných v iných IT systémoch, najmä ak sa používa digitálne vybavenie a softvér. Bez ohľadu na vybraté riešenie však prevádzkovateľ musí primerane chrániť všetky komponenty systému video monitorovania a údaje vo všetkých fázach, t. j. počas ukladania (údaje v pokoji), prenosu (údaje v tranzite) a spracovania (používané údaje). Preto je potrebné, aby prevádzkovatelia a spracovatelia kombinovali organizačné a technické opatrenia.

22 WP 168, Stanovisko na tému „Budúcnosť súkromia“, spoločný príspevok Pracovnej skupiny pre ochranu údajov a Pracovnej skupiny pre políciu a spravodlivosť ku konzultácii s Európskou komisiou o právnom rámci pre základné právo na ochranu osobných údajov (Schválené 1. decembra 2009).

|  |  |
| --- | --- |
| Schválené | 30 |

1. Pri výbere technických riešení by prevádzkovateľ mal brať do úvahy technológie priateľské voči súkromiu aj preto, že zvyšujú bezpečnosť. Príkladom takýchto technológií sú systémy, ktoré pri poskytovaní videozáznamu dotknutým osobám umožňujú maskovanie alebo vyšrafovanie oblastí, ktoré nie sú relevantné pre daný záznam, a úpravu obrazov, na ktorej sa nachádzajú tretie osoby.23 Na druhej strane by vybraný systém nemal poskytovať funkcie, ktoré nie sú potrebné (napr. neobmedzený pohyb kamier, schopnosť priblíženia, rádiový prenos, analýza a zvukové záznamy). Funkcie, ktoré nie sú potrebné, musia byť deaktivované.

K tejto téme je k dispozícii mnoho literatúry, vrátane medzinárodných noriem a technických špecifikácií o fyzickej bezpečnosti multimediálnych systémov24a bezpečnosti všeobecných IT systémov25. Táto časť preto poskytuje iba prehľad tejto témy na vysokej úrovni.

9.3.1 Organizačné opatrenia

1. Okrem prípadných potrebných DPIA (pozri oddiel 10) by prevádzkovatelia mali pri vytváraní svojich vlastných pravidiel a postupov týkajúcich sa videa zohľadniť tieto témy:
	* Kto je zodpovedný za správu a prevádzku systému video monitorovania.
	* Účel a rozsah projektu video monitorovania.
	* Primerané a zakázané použitie (kde a kedy je povolené video a kde a kedy nie; napr. Použitie skrytých kamier a zvuku okrem záznamu videa)26.
	* Opatrenia na zabezpečenie transparentnosti uvedené v oddiele 7 *(Povinnosti týkajúce sa transparentnosti a informovania).*
	* Opatrenia na zabezpečenie transparentnosti uvedené v oddiele 7 (Povinnosti týkajúce sa transparentnosti a informovania).
	* Kto musí absolvovať príslušné školenie a kedy.
	* Kto má prístup k videozáznamom a na aké účely.
	* Prevádzkové postupy (napr. kto a odkiaľ monitoruje video, čo robiť v prípade incidentu týkajúceho sa porušenia ochrany údajov).
	* Aké postupy musia externé strany dodržiavať, ak chcú požiadať o videonahrávky, a postupy zamietnutia alebo udelenia takýchto žiadostí.
	* Postupy pri obstarávaní, inštalácii a údržbe VSS.
	* Postupy riadenia a obnovy po incidente.

9.3.2 Technické opatrenia

1. **Bezpečnosť systému** znamená **fyzickú bezpečnosť** všetkých komponentov systému a integritu systému, t. j. **ochranu pred úmyselným a neúmyselným zasahovaním do jeho normálnych operácií a kontrolu prístupu** **a odolnosť proti nim**. Bezpečnosť údajov znamená **dôvernosť** (údaje sú prístupné iba tým, ktorým bol udelený prístup), **integrita** (prevencia proti strate údajov alebo manipulácii s nimi) a **dostupnosť** (údaje sú prístupné, keď sa to vyžaduje).

23 Používanie takýchto technológií môže byť v niektorých prípadoch dokonca povinné, aby sa dosiahol súlad s článkom 5 ods. 1 písm. c). V každom prípade môžu slúžiť ako príklady osvedčených postupov.

24 IEC TS 62045 — Multimediálna bezpečnosť - Usmernenie na ochranu súkromia zariadení a systémov používaných a nepoužívaných.

25 ISO/IEC 27000 — Séria systémov riadenia informačnej bezpečnosti. 26 To môže závisieť od vnútroštátnych zákonov a sektorových predpisov.

Schválené 31

1. **Fyzická bezpečnosť** je nevyhnutnou súčasťou ochrany údajov a prvej línie obrany, pretože chráni zariadenie VSS pred krádežou, vandalizmom, prírodnou katastrofou, katastrofami spôsobenými ľudskou činnosťou a náhodným poškodením (napr. pred elektrickým prepätím, extrémnymi teplotami a rozliatou kávou). V prípade analógových systémov hrá hlavnú úlohu pri ich ochrane fyzická bezpečnosť.
2. **Bezpečnosť systému a údajov,** t.j.ochrana proti úmyselnému a neúmyselnému zasahovaniu do jej normálnej činnosti zahŕňa:
	* Ochrana celej infraštruktúry VSS (vrátane vzdialených kamier, kabeláže a napájania) proti fyzickému poškodeniu a krádeži.
	* Ochrana prenosu záberov pomocou komunikačných kanálov zabezpečených proti odpočúvaniu.
	* Šifrovanie údajov.
	* Používanie hardvérových a softvérových riešení, ako sú brány firewall, antivírusové systémy alebo systémy na detekciu narušenia proti počítačovým útokom.
	* Zisťovanie porúch komponentov, softvéru a prepojení.
	* Prostriedky na obnovenie dostupnosti a prístupu do systému v prípade fyzického alebo technického incidentu.
3. **Kontrola prístupu** zabezpečuje, že prístup k systému a údajom majú iba oprávnení ľudia, zatiaľ čo ostatní to nemôžu robiť. Medzi opatrenia, ktoré podporujú kontrolu fyzického a logického prístupu, patria:
	* Zabezpečenie, aby všetky priestory, v ktorých sa vykonáva monitorovanie prostredníctvom videa a kde sa ukladajú videozáznamy, boli zabezpečené proti neoprávnenému prístupu tretích strán.
	* Umiestnenie polohovacích monitorov takým spôsobom (najmä ak sú na otvorenom priestranstve, napríklad na recepcii), aby si ich mohli prezerať iba oprávnení operátori.
	* Postupy udeľovania, zmeny a zrušenia fyzického a logického prístupu musia byť definované a presadzované.
	* Metódy a prostriedky autentifikácie a autorizácie používateľov, napr. implementuje sa dĺžka hesiel a frekvencia zmien.
	* Akcie vykonávané používateľom (do systému aj do údajov) sa zaznamenávajú a pravidelne preverujú.
	* Monitorovanie a zisťovanie zlyhaní prístupu sa vykonáva nepretržite a zistené nedostatky sa riešia čo najskôr.

|  |  |
| --- | --- |
| Schválené | 32 |

10 POSÚDENIE VPLYVU NA OCHRANU ÚDAJOV

1. Podľa článku 35 ods. 1 sa od prevádzkovateľov GDPR vyžaduje, aby vykonávali posúdenie vplyvu na ochranu údajov (DPIA), ak je pravdepodobné, že spôsob spracovania údajov bude mať za následok vysoké riziko pre práva a slobody fyzických osôb. V článku 35 ods. 3 písm. C) GDPR sa stanovuje, že prevádzkovatelia sú povinní vykonávať kontrolu údajov na ochranu údajov, ak spracovanie predstavuje systematické monitorovanie vo verejnom priestore vo veľkom rozsahu. Okrem toho sa podľa článku 35 ods. 3 písm. B) vyžaduje, aby prevádzkovateľ zamýšľal spracovávať osobitné kategórie údajov vo veľkom rozsahu.
2. Usmernenia na posúdenie vplyvu na ochranu údajov27 poskytujú ďalšie rady a podrobnejšie príklady týkajúce sa video monitorovania (napr. týkajúce sa „použitia kamerového systému na monitorovanie jazdného správania na diaľniciach“). V článku 35 ods. 4 GDPR sa vyžaduje, aby každý dozorný orgán uverejnil zoznam druhov operácií spracovania, ktoré podliehajú povinnému DPIA v ich krajine. Tieto zoznamy sa zvyčajne nachádzajú na webových stránkach orgánov. Vzhľadom na typické účely videozáznamu (ochrana ľudí a majetku, odhaľovanie, prevencia a kontrola trestných činov, zhromažďovanie dôkazov a biometrická identifikácia podozrivých) je odôvodnené predpokladať, že v mnohých prípadoch videozáznamu sa bude vyžadovať DPIA. Z tohto dôvodu by prevádzkovatelia údajov mali tieto dokumenty dôkladne nahliadnuť, aby sa zistilo, či je takéto posúdenie potrebné, a v prípade potreby ich vykoná. Výsledok vykonaného DPIA by mal určiť prevádzkovateľovu voľbu implementovaných opatrení na ochranu údajov.
3. Je tiež dôležité poznamenať, že ak výsledky DPIA naznačujú, že spracovanie by napriek bezpečnostným opatreniam plánovaným prevádzkovateľom malo za následok vysoké riziko, bude pred spracovaním potrebné konzultovať s príslušným dozorným orgánom. Podrobnosti o predchádzajúcich konzultáciách možno nájsť v článku 36.

Za Európsky výbor pre ochranu údajov predseda

(Andrea Jelinek)

1. WP248 rev.01, Usmernenia k posúdeniu vplyvu na ochranu údajov (DPIA) a určovaní, či spracovanie „bude mať pravdepodobne za následok vysoké riziko“ na účely Nariadenia 2016/679. - schválené EDPB

|  |  |
| --- | --- |
| Schválené | 33 |