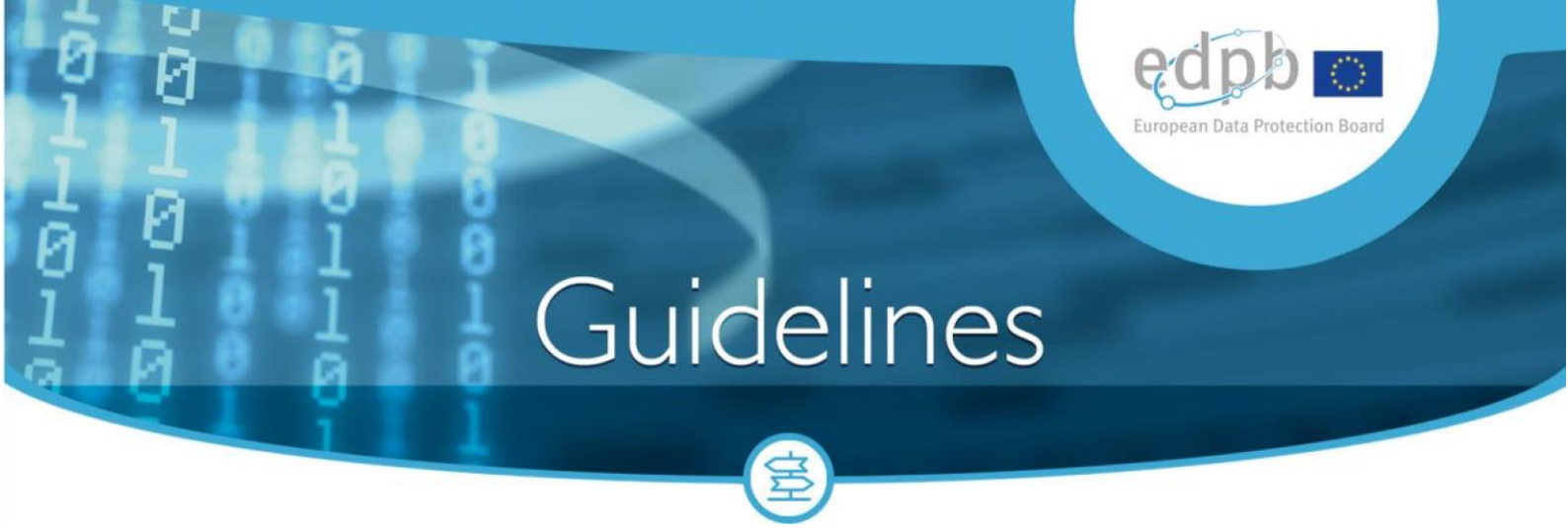


Neoficiální překlad

Plenární zasedání Evropského sboru pro ochranu osobních údajů (EDPB) 9-10. července 2019

Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím video zařízení

Verze pro veřejnou konzultaci

Schváleno 10. července 2019

Obsah

Evropský sbor pro ochranu osobních údajů

S ohledem na článek 70 (1e) nařízení 2016/679/EU Evropského parlamentu a Rady ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, (dálen jen „GDPR“),

S ohledem na smlouvu o EHP a zejména její přílohu XI a protokol 37 ve znění rozhodnutí společného výboru EHP č. 154/2018 ze dne 6. července 2018,

S ohledem na článek 12 a článek 22 svého jednacího řádu ze dne 25, května 2018, revidovaného dne 23. listopadu 2018,

SCHVÁLIL NÁSLEDUJÍCÍ POKYNY

1 ÚVOD

1. Intenzivní užívání videozařízení ovlivňuje chování občanů. Rozsáhlé zavádění takových nástrojů do mnoha oblastí lidského života vytváří novou formu tlaku na jednotlivce, který má snahu bránit se odhalení všeho, co by mohlo být vnímáno jako anomálie. Ve skutečnosti mohou tyto technologie omezovat možnost anonymního pohybu či anonymního využívání služeb a v obecné rovině omezovat možnost zůstat nepozorován. Dopady z hlediska ochrany dat jsou masivní.

2. Zatímco jednotlivci nemusí mít problém např. s videosledováním pro určité bezpečnostní účely, musí být poskytnuty záruky zabraňující jakémukoliv zneužití pro zcela odlišné a pro subjekt údajů nepředpokládané účely (např. marketing, sledování výkonu zaměstnance apod.). Kromě toho v současnosti existuje mnoho nástrojů využití kamerových záznamů a tradiční kamery jsou nahrazovány kamerami chytrými. Množství dat vytvářených prostřednictvím videa, v kombinaci s uvedenými nástroji a technikami, zvyšuje riziko druhotného využití (ať již v souvislosti s původně stanoveným účelem či nikoliv) nebo dokonce riziko zneužití. Obecné zásady GDPR (článek 5) by proto měly být vždy pečlivě zvažovány při nakládání s videosledováním.

3. Systémy videosledování v mnoha směrech mění způsob, jakým profesionálové ze soukromého a veřejného sektoru postupují na soukromých i veřejných místech za účelem zvýšení bezpečnosti, analýzy návštěvnosti, zprostředkování personalizované reklamy atd. Videosledování se stalo vysoce účinným díky rostoucímu uplatňování inteligentní analýzy kamerových záznamů. Tyto techniky mohou být více (komplexní biometrické technologie) či méně rušivé (např. jednoduchý výpočetní algoritmus). Zůstat anonymní a chránit své soukromí je stále obtížnější. Otázky ochrany dat se svou povahou mohou lišit případ od případu, stejně jako právní analýza při využívání té či oné technologie.

4. Kromě problémů s ochranou soukromí existují také rizika spojená s poruchami těchto zařízení a předsudky, které mohou vyvolat. Vědci informují o tom, že software používaný k identifikaci podle obličeje, k rozpoznávání nebo analýze se chová odlišně v závislosti na věku, pohlaví a etnickém původu identifikované osoby. Algoritmy fungují odlišně na základě různých demografických prvků, takže hrozí, že zaujatost v rozpoznávání podle obličeje bude posilovat společenské předsudky. Proto také musí správci zajistit, aby biometrické zpracování dat odvozených z videosledování bylo předmětem pravidelného hodnocení jeho relevance a dostatečnosti poskytovaných záruk.

5. Kamerové sledování není automaticky nezbytné, pokud existují jiné způsoby dosažení daného účelu. V opačném případě riskujeme změnu kulturních norem, která povede k akceptaci nedostatku soukromí jako obecného východiska.

6. Cílem těchto pokynů je poskytnout návod, jak uplatnit GDPR při zpracování osobních údajů prostřednictvím videozařízení. Příklady nejsou vyčerpávající. Obecné zdůvodnění může být použito pro všechny oblasti připadající v úvahu.

2 ROZSAH PŮSOBNOSTI[1]

2.1 Osobní údaje

7. Systematické automatizované monitorování konkrétního prostoru optickými nebo audiovizuálními prostředky, většinou z důvodu ochrany majetku nebo života či zdraví jednotlivce, se stalo významným fenoménem dnešní doby. Tato činnost s sebou přináší shromažďování a uchovávání obrazových nebo audiovizuálních informací o všech osobách vstupujících do sledovaného prostoru, které jsou identifikovatelné podle jejich vzhledu nebo jiných specifických prvků. Totožnost těchto osob lze zjistit na základě těchto prvků. Umožňuje také také další zpracování osobních údajů vypovídajících o přítomnosti osoby a jejím chování ve sledovaném prostoru. Možné riziko zneužití těchto údajů roste s rozsahem monitorovaného prostoru a s počtem osob, které se v něm pohybují. Tuto skutečnost zohledňuje GDPR v článku 35 (3) (c), který vyžaduje provedené posouzení vlivu na ochranu osobních údajů v případě rozsáhlého systematického monitorování veřejně přístupných prostor, stejně jako článek článek 37 (1) (b), který požaduje, aby zpracovatelé určili pověřence pro ochranu osobních údajů, pokud operace zpracování vyžadují kvůli své povaze pravidelné a systematické monitorování subjektů údajů.

8. GDPR se však nevztahuje na zpracování dat, která nemají vztah k nějaké osobě, např. pokud nelze jednotlivce přímo nebo nepřímo identifikovat.

> Příklad: GDPR se nevztahuje na atrapy - falešné kamery (tj. kamery, které nefungují jako skutečná kamery, takže jejich prostřednictvím nejsou zpracovávány žádné osobní údaje). *V některých členských státech však tato otázka může podléhat jiné právní úpravě.*
>
> Příklad: Na záznamy z velkých výšek se GDPR vztahuje jen, pokud lze zpracovávaná data přiřadit ke konkrétní osobě.
>
> Příklad: Videokamera je zabudovaná v autě jako parkovací asistent. Pokud je taková kamera konstruovaná nebo nastavená tak, aby neshromažďovala žádné informace týkající se fyzických osob (poznávací značky nebo informace, které by mohly vést k identifikace kolemjdoucích), pak se GDPR neuplatní.

9.

2.2 Aplikace trestněprávní směrnice, LED (EU2016/680)

10. Zpracování osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů včetně zabezpečení a prevence před hrozbami pro veřejnou bezpečnost, spadá pod směrnici EU 2016/680.

[1] EDPB poznamenává, že pokud to GDPR umožňuje, mohou se uplatnit konkrétní ustanovení vnitrostátní legislativy.

2.3 Domácí výjimka

11. Podle článku 2 (2) (c) spadá mimo rozsah GDPR zpracování osobních údajů fyzickou osobou v průběhu výlučně osobních či domácích činností, což může zahrnovat i činnosti online.[2]

12. Toto ustanovení – takzvaná domácí výjimka – musí být v kontextu kamerového sledování vykládáno úzce. Proto, jak konstatoval Evropský soudní dvůr, musí tzv. „domácí výjimka" být „*vykládána tak, že se týká pouze činností prováděných v rámci soukromého nebo rodinného života jednotlivců, což zjevně neplatí pro zpracování osobních údajů, jež spočívá v jejich zveřejnění na internetu tak, že se zpřístupní neomezenému počtu osob*"[3]. Kromě toho, pokud systém videosledování v rozsahu, v němž umožňuje stálý záznam a ukládání osobních údajů, zabírá „*třebaže částečně – veřejné prostranství, a je tudíž zaměřen mimo soukromou sféru osoby, která jeho prostřednictvím zpracovává údaje, nelze jeho provozování považovat za výlučně „osobní či domácí" činnost ve smyslu čl. 3 odst. 2 druhé odrážky směrnice 95/46."* [4]

13. Pokud jde o videozařízení provozované uvnitř prostor soukromé osoby, může spadat pod domácí výjimku. To bude záviset na několika faktorech, které je všechny nutno vzít v úvahu. Kromě výše uvedených okolností zmíněných v rozsudcích ESD musí uživatel zařízení pro kamerové sledování doma zohlednit, zda má nějaký osobní vztah k subjektu údajů, zda rozsah a četnost sledování mohou být považovány za určitý druh profesionální aktivity provozovatele a zda sledování může mít nežádoucí dopad na subjekty údajů. Přítomnost jednoho z vyjmenovaných faktorů ještě nutně neznamená, že zpracování nespadá pod domácí výjimku, pro definitivní určení je nutné provést celkové posouzení.

[2] Viz také recitál 18.

[3] Evropský soudní dvůr, rozsudek v případu C-101/01, *Bodil Lindqvist case*, 6. listopadu 2003, odst. 47.

[4] Evropský soudní dvůr, rozsudek v případu C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, 11. prosince 2014, odst. 33.

Příklad: Turista pořizuje videozáznamy mobilním telefonem a tak, aby zdokumentoval svou dovolenou. Záznamy ukáže svým přátelům a rodině, nezpřístupní je však neurčitému počtu lidí. Na tento případ se domácí výjimka vztahuje.

Příklad: Cyklistka na horském kole chce zaznamenat svůj sjezd akční kamerou. Jede odlehlou krajinou a záznamy hodlá použít jen pro osobní potřebu doma. I na tento případ se vztahuje domácí výjimka.

Příklad: Majitel monitoruje svoji zahradu a pořizuje záznam. Pozemek je oplocen a pouze sám majitel (správce dat) a jeho rodina chodí pravidelně na zahradu. Na tuto situaci se domácí výjimka bude vztahovat za předpokladu, že kamerové zařízení nebude ani částečně zabírat veřejné prostranství nebo sousedící pozemek.

14.

3 ZÁKONNOST ZPRACOVÁNÍ

15. Před užitím osobních údajů je třeba přesně stanovit účely (článek 5 (1) (b)). Kamerové sledování může sloužit řadě účelů, např. ochraně majetku či jiného vlastnictví nebo shromáždění důkazů pro občanskoprávní spor.[5] Tyto účely sledování by měly být písemně dokumentovány (Článek 5 (2)) a je potřebné je upřesnit pro každou použitou kameru. Kamery používané pro stejný účel jedním správcem mohou být dokumentovány společně, pokud každá z kamer slouží uvedenému účelu. Dále musí být subjekty údajů informovány o účelu/účelech zpracování v souladu s článkem 13 (*viz kapitola 7 Transparentnost a informační povinnost*). Videosledování založené na pouhém účelu „bezpečnost“ nebo „pro vaší bezpečnost“ není dostatečně konkrétní (Článek 5 (1) (b)). Kromě toho je to v rozporu se zásadou zpracování osobních údajů zákonným, korektním a transparentním způsobem ve vztahu k subjektu údajů (viz článek 5 (1) (a)).

16. V podstatě každý zákonný důvod podle článku 6 (1) může poskytnout právní základ pro zpracování dat z videosledování. Například článek 6 (1) (c) se použije, pokud vnitrostátní právo stanoví povinnost videosledování.[6] V praxi však budou pravděpodobně nejpoužívanější ustanovení

- článek 6 (1) (f) (oprávněný zájem);
- článek 6 (1) (e) (nutnost provést úkol prováděný ve veřejném zájmu nebo pří výkonu veřejné moci).

Ve zcela výjimečných případech může správce použít jako právní základ článek 6 (1) (a) (souhlas).

3.1 Oprávněný zájem, článek 6 (1) (f)

17. Právní posouzení podle článku 6 (1) (f) by mělo být založeno na následujících kritériích v souladu s recitálem 47.

[5] Pravidla pro shromažďování důkazů pro civilní žaloby se v členských zemích liší.

[6] Tyto pokyny neanalyzují nebo nejdou do podrobností ohledně vnitrostátního práva, které se v členských zemích může lišit.

3.1.1 Existence oprávněných zájmů

18. Videosledování je zákonné, pokud je nezbytné k naplnění účelu oprávněného zájmu správce nebo třetí strany, pokud však nad těmito zájmy nepřevažují zájmy nebo základní práva a svobody subjektů údajů (článek 6 (1) (f)). Oprávněné zájmy sledované správcem nebo třetí stranou mohou být zákonné, [7] hospodářské nebo nemateriální.[8] Správce by však měl zvážit, že pokud subjekt údajů vznese námitku vůči sledování podle článku 21, může správce nadále pokračovat ve videosledování subjektu údajů jen, pokud jde o *závažný* oprávněný zájem, který převažuje nad zájmy, právy a svobodami subjektu údajů nebo slouží k určení, výkonu nebo obhajobě právních nároků.

19. V podmínkách reálné a riskantní situace může účel ochrany majetku proti vloupání, krádeži nebo vandalismu zakládat oprávněný zájem pro videosledování.

20. Oprávněný zájem musí být skutečný a musí být aktuální (tj. nesmí být fiktivní nebo spekulativní).[9]Musí existovat skutečně obtížný a reálný životní problém jako např. vznik škody nebo vážný incident v minulosti, před zahájením sledování. S ohledem na zásadu odpovědnosti by se správcům mělo doporučit, aby zdokumentovali relevantní incidenty (datum, způsob, finanční ztrátu) a související trestní obvinění. Takto doložené události mohou být silným důkazem pro existenci oprávněného zájmu.

> Příklad: Majitel obchodu chce otevřít novou prodejnu a hodlá nainstalovat systém videosledování. Pomocí statistiky může prokázat, že v okolí existuje vysoký předpoklad vandalismu. Užitečné jsou rovněž skutečnosti z okolních obchodů. Není nezbytné, aby správci vznikla škoda. Není však dostačující předložit národní nebo obecnou statistiku trestné činnosti, aniž by byla analyzována daná oblast nebo nebezpečí pro tento konkrétní obchod.

21.

22. Bezprostřední ohrožení může zakládat oprávněný zájem např. u obchodů prodávajících cenné zboží (např. klenotnictví) nebo na místech, která jsou typická pro určité majetkové trestné činy (např. čerpací stanice).

23. GDPR rovněž jasně uvádí, že veřejné orgány nemohou u svého zpracování spoléhat na důvod oprávněného zájmu, pokud plní své úkoly, viz článek 6 (1) věta 2.

3.1.2 Nezbytnost zpracování

24. Osobní údaje by měli být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány (minimalizace údajů), viz článek 5 (1) (c). Předtím než správce instaluje systém kamerového sledování, vždy by měl kriticky prozkoumat, zda je takové opatření jednak vhodné k dosažení požadovaného cíle, jednak, zda je přiměřené a nezbytné pro dané účely. Prostředky videosledování by měly být zvoleny pouze, pokud nelze účel zpracování rozumně naplnit jinými způsoby, které jsou méně rušivé z hlediska základních práv a svobod subjektu údajů.

25. Chce-li správce chránit svůj majetek před majetkovými trestnými činy, může také namísto nainstalování systému videosledování provést alternativní bezpečnostní opatření jako například oplotit pozemek, zavést pravidelné pochůzky, využívat vrátné, poskytnout lepší osvětlení, zavést bezpečnostní zámky, nerozbitná okna a dveře nebo použít nátěry odolné vůči graffiti či nástěnné folie. Tato opatření mohou být stejně účinná proti vloupání, krádeži nebo vandalismu jako videosystémy.

---

[7] Evropský soudní dvůr, rozsudek v případě C-13/16, *Rīgas satiksme case*, 4. květen 2017

[8] Viz wp 217, Pracovní skupina pro článek 29, str. 24 a násl.

[9] Viz wp 217, Pracovní skupina pro článek 29, str. 24 a násl.

26. Před zavedením videosystému je správce povinen posoudit kde a kdy jsou opatření videosůedování skutečně nutná. Obvykle kamerový systém provozovaný v noci či mimo pracovní dobu splní potřebu správce předcházet ohrožení svého majetku.

27. Obecně končí nezbytnost použití videosledování k ochraně prostor správce na hranici jeho pozemku.[10] Existují však případy, kdy sledování majetku nedostačuje k účinné ochraně. V některých jednotlivých případech může být nezbytné rozšířit videosledování i na prostory v bezprostředním okolí. V této souvislosti by správce měl zvážit použití fyzických nebo technických prostředků, například blokovat nebo rozostřit nerelevantní prostory.

> Příklad: Knihkupectví hodlá chránit své prostory před vandalismem. Obecně by kamery měly snímat jen prostory samotné, neboť pro tento účel není nezbytné sledovat okolní nebo veřejné plochy v sousedství obchodu.

28.

29. V souvislosti s nezbytností zpracování vyvstávají také otázky způsobu, jakým jsou uchovávány důkazy. V některých případech může být nezbytné použít řešení na způsob černé skříňky, kde je záznam automaticky po určité době mazán a je přístupný jen v případě incidentu. Jindy nemusí být nezbytné pořizovat videozáznam a bude vhodnější sledování v reálném čase. Rozhodování mezi černou skříňkou a monitorováním v reálném čase by mělo vycházet ze stanového účelu. Pokud je například účelem videodohledu uchování důkazů, pak sledování v reálném čase není vhodné. Někdy může být sledování v reálném čase rušivější než uchovávání a automatické mazání záznamu ve stanovených intervalech. Zásada minimalizace údajů musí být v této souvislosti respektována (článek 5 (1) (c)). Nemělo by se také zapomínat, že správce může namísto kamer využít bezpečnostní personál, který je schopen okamžitě reagovat a zasáhnout.

3.1.3 Vyvažování zájmů

30. Za předpokladu, že videosledování je nezbytné k ochraně oprávněných zájmů správce, může být videosystém uveden do provozu pouze tehdy, pokud oprávněné zájmy správce nebo třetí strany (např. ochrany majetku nebo osobní integrity) nejsou převáženy zájmy nebo základními právy a svobodami subjektu údajů. Správce musí zvážit 1) do jaké míry se sledování dotkne oprávněných zájmů, základních práv a svobod jednotlivců, a 2) zda to nezpůsobí nějaké narušení či nežádoucí důsledky z hlediska práv subjektu údajů. Vyvažování zájmů je v podstatě povinné. Základní práva a svobody na jedné straně a oprávněné zájmy správce na druhé straně musí být pečlivě vyhodnoceny a vyváženy.

[10] To by mohlo být v některých členských státech předmětem vnitrostátní legislativy.

Příklad: Soukromá společnost provozující parkoviště zdokumentovala opakující se problémy s krádežemi v zaparkovaných autech. Prostor parkoviště je otevřený a kdokoliv do něj může snadno dostat, je však jasně označen značkami a zátarasy po celém obvodu. Firma má oprávněný zájem (prevence krádeží v autech zákazníků) monitorovat prostor během denní doby, kdy lze podle zkušenosti očekávat potíže. Subjekty údajů jsou sledovány během omezeného časového intervalu, nenacházejí se v prostorech pro rekreační využití a je také v jejich zájmu, aby se krádežím předcházelo. Zájem subjektů údajů nebýt sledován je v tomto případě převážen oprávněným zájmem správce.

Příklad: Restaurace se rozhodne rozmístit kamery na toaletách za účelem kontroly čistoty sanitárního zařízení. V tomto případě práva subjektu údajů jasně převažují nad zájmem správce, proto kamery nemohou být instalovány.

31.

3.1.3.1 Rozhodování případ od případu

32. Vzhledem k tomu, že vyvažování zájmů je podle obecného nařízení povinné, je třeba rozhodovat případ od případu (viz článek 6 (1) (f)). Odkazování na abstraktní situace nebo srovnávání podobných případů je nedostatečné. Správce musí vyhodnotit rizika zásahu do práv subjektu údajů; rozhodujícím kritériem je zde intenzita zásahu do práv a svobod jednotlivce.

33. Intenzita může být mimo jiné definována typem shromažďovaných informací (informační obsah), rozsahem (informační hustota, prostorový a zeměpisný rozsah), počtem dotčených subjektů údajů, ať již v absolutním vyjádření nebo jako podíl příslušné populace, danou situací, aktuálními zájmy skupiny subjektů údajů, alternativními prostředky, jakož i povahou a rozsahem hodnocení údajů.

34. Důležitými vyvažovacími faktory může být velikost sledovaného území a počet monitorovaných subjektů údajů. Použití kamerového dohledu v odlehlé oblasti (např. pro pozorování života divokých zvířat nebo k ochraně kritické infrastruktury jako třeba soukromá radiová anténa) musí být posuzováno jinak než videosledování v pěší zóně nebo v obchodním centru.

Příklad: Pokud je instalována kamera v autě (např. za účelem shromažďování důkazů pro případ nehody), je důležité zajistit, aby tato kamera nezaznamenávala nepřetržitě provoz, stejně tak jako osoby poblíž silnice. V opačném případě zájem mít kamerový záznam jako důkaz ve spíše teoretickém případě dopravní nehody nemůže odůvodnit závažný zásah do práv subjektu údajů.[11]

3.1.3.2 Důvodná očekávání subjektu údajů

35. Podle recitálu 47 je třeba existenci oprávněného zájmu pečlivě posoudit. Zde musí být zohledněno přiměřené očekávání subjektu údajů v době a v kontextu zpracování osobních dat. Pokud jde o systematické monitorování, vztah mezi subjektem údajů a správcem může mít různé podoby a může významně ovlivňovat případná přiměřená očekávání subjektu údajů. Výklad konceptu přiměřeného očekávání by neměl být založen pouze na subjektivních očekáváních v dané věci. Rozhodujícím kritériem musí být spíše okolnost, zda objektivně třetí strana může důvodně očekávat a dovodit, že bude v dané konkrétní situaci subjektem sledování.

36. Například, zaměstnanec na pracovišti nebude ve většině případů předpokládat, že je monitorován zaměstnavatelem.[12] Dále není monitorování očekáváno na vlastní zahradě, v obytných oblastech nebo na

[11] I když za určitých okolností je teoreticky možné určit právní základ pro části takového sledování, správce ejně musí dodržet obecné zásady (článek 5 GDPR) a povinnosti týkající se transparentnosti a náležitého informování subjektu údajů (čl. 13 GDPR).

[12] Viz též Pracovní skupina 29, Stanovisko 2/2017 ke zpracování dat na pracovišti, WP 249, přijato 8. června 2017.

ošetřovně. Obdobně není důvodné očekávat monitorování v sanitárních zařízeních nebo v saunách – monitorování na takových místech je intenzivním narušením práv subjektu údajů. Subjekty údajů důvodně očekávají, že na takových místech nebudou sledováni prostřednictvím kamer. Na druhé straně zákazník banky by mohl očekávat, že bude monitorován uvnitř banky uvnitř banky nebo u bankomatu.

37. Subjekty údajů mohou také očekávat, že nebudou monitorovány ve veřejných prostorách, zejména v těch, které jsou typicky využívány k odpočinku, regeneraci nebo volnočasovým aktivitám, stejně jak na místech, kde se jednotlivci zdržují nebo komunikují, jako jsou prostory k sezení, stoly v restauraci, parky, kina a fitnesscentra. V těchto případech často převáží oprávněný zájem nebo práva a svobody subjektu údajů nad legitimním zájmem správce.

> Příklad: Subekt údajů neočekává, že bude monitorován v protoru toalet. Například videosledování za účelem prevence úrazů není na těchto místech přiměřené.

38.

39. Symboly informující subjekt údajů o videosledování nejsou relevantní z pohledu určení, co subjekt údajů může objektivně očekávat.

3.2Nezbytnost splnit úkol prováděný ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen, článek 6 (1) (e)

40. Osobní údaje mohou být podle článku 6 (1) (e) zpracovávány prostřednictvím videosledování, pokud je to nezbytné ke splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci.[13] Může nastat situace, že výkon veřejné moci sice takové zpracování sice neumožní, avšak jiné právní důvody jako „zdraví a bezpečnost“ k ochraně zaměstnanců nebo návštěvníků mohou umožnit zpracování v omezené míře, přičemž je třeba mít stále na zřeteli povinnosti podle GDPR a práva subjektů údajů.

41. Členské státy mohou zachovat nebo zavést zvláštní vnitrostátní legislativu pro videosledování v souladu s pravidly GDPR, která odrobněji stanoví konkrétní požadavky na zpracování v souladu se zásadami stanovenými v GDPR (např. omezená doba uchovávání, přiměřenost).

3.3 Souhlas, článek 6 (1) (a)

42. Souhlas musí být svobodný, konkrétní, informovaný a jednoznačný projev vůle, jak je to popsáno v pokynech k souhlasu.[14]

43. V případě systematického monitorování platí, že souhlas subjektu údajů může sloužit jako právní základ v souladu s článkem 7 (viz recitál 43) jen ve výjimečných případech. K povaze videosledování patří, že současně monitoruje neznámý počet lidí. Správce bude stěží schopen prokázat, že subjekt údajů udělil souhlas před

[13] Důvod pro zmíněné zpracování by měl být stanoven unijním právem nebo legislativou členského státu a má být nezbytný pro výkon úkolu vykonávaného ve veřejném zájmu nebo při výkonu veřejné moci svěřené správci (článek 6 (3)).
[14] Kromě toho přijala Pracovní skupina WP29 „Pokyny k souhlasu podle nařízení 2016/679“ (WP 259 rev. 01), které by také mělo být vzato v úvahu.

zpracováním svých osobních údajů (článek 7 (1)). A za předpokladu, že subjekt údajů svůj souhlas odvolá, bude pro správce obtížné doložit, že příslušná data nebudou nadále zpracovávána (článek 7 (3)).

> Příklad: Atleti mohou požadovat, aby byli monitorování během individuálního cvičení za účelem analýzy techniky a výkonu. Na druhé straně, pokud sportovní klub převezme iniciativu a rozhodne se, že bude pro stejný účel monitorovat celé družstvo, nemusí vždy být souhlas platný, neboť jednotliví atleti se mohou cítit pod tlakem udělit souhlas, aby jejich odmítnutí nemělo negativní dopad na ostatní členy týmu.

44.

45. Pokud se správce chce spolehnout na souhlas, je povinen zajistit, aby každý subjekt údajů vstupující do monitorovaného prostoru předem udělil souhlas. Tento souhlas musí splňovat podmínky podle článku 7. Vstup do označeného monitorovaného prostoru (např. lidé jsou vyzváni projít určitým vstupním prostorem nebo branou do sledovaného prostoru), nepředstavuje vyjádření nebo jasný potvrzující úkon potřebný pro souhlas, pokud nejsou splněna kritéria podle článku 4 a 7, jak jsou popsána v pokynech k souhlasu.[15]

46. Vzhledem k nerovnováze moci mezi zaměstnavatelem a zaměstnancem se zaměstnavatel ve většině případů nemůže spolehnout na souhlas ke zpracování osobních údajů, protože je nepravděpodobné, že by byl udělen svobodně. Pokyny k souhlasu by měly být zvažovány v tomto kontextu.

47. Právo členských států nebo kolektivní dohody včetně „pracovních smluv“ mohou stanovit konkrétní pravidla pro zpracování osobních údajů zaměstnanců v zaměstnaneckém kontextu (viz čl. 88).

4 ZPŘÍSTUPNĚNÍ VIDEOZÁZNAMŮ TŘETÍM STRANÁM

48. Obecně platí, že obecná právní úprava GDPR se vztahuje na zpřístupnění videozáznamů třetím stranám.

4.1 Zpřístupnění videozáznamů třetím stranám

49. Zpřístupnění je definováno v článku 4 (2) jako přenos (např. individuální sdělení), šíření (např. uveřejnění online) nebo jakékoliv jiné zpřístupnění. Pojem třetí strany je definován v článku 4 (10). Pokud se uskutečňuje zpřístupnění do třetí země nebo mezinárodní organizace, uplatní se také zvláštní ustanovení článku 44 a následujících.

50. Jakékoliv zpřístupnění osobních údajů je samostatný druh zpracování osobních údajů, pro které správce potřebuje právní důvod podle článku 6.

> Příklad: Správce, který hodlá umístit záznam na internet, potřebuje k takovému zpracování právní důvod, například získáním souhlasu od subjektu údajů podle článku 6 (1) (a).

51.

[15] Recitál 51 tuto analýzu podporuje, když uvádí, že *„zpracování fotografií by nemělo být systematicky považováno za zpracování zvláštních kategorií osobních údajů, neboť na fotografie se definice biometrických údajů vztahuje pouze v případech, kdy jsou zpracovávány zvláštními technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby“*.

52. Přenos videozáznamu třetím stranám za jiným účelem, než pro který byl pořízen, je možný podle pravidel článku 6 (4).

> Příklad: Videosledování zábrany (na parkovišti) je nainstalováno za účelem řešení případných škod. Dojde ke škodě a záznam je předán právníkovi k řešení případu. Účel záznamu je totožný s účelem předání.
>
> Příklad: Zábrana (na parkovišti) je sledována kamerou za účelem řešení škod. Záznam je zveřejněn na internetu čistě za účelem pobavení. V tomto případě došlo ke změně účelu, který není v souladu s prvotním účelem. Dále by pro takové zpracování (zveřejnění) bylo problematické stanovit odpovídající účel.

53.

54. Příjemce třetí strany musí provést vlastní právní analýzu, především určit právní základ pro své zpracování podle článku 6 (např. obdržení daného materiálu).

4.2 Zpřístupnění videozáznamů donucovacím orgánům

55. Zpřístupnění videozáznamu donucovacím orgánům je také samostatný proces vyžadující samostatné odůvodnění ze strany správce.

56. Podle článku 6 (1) (c) je zpracování zákonné, pokud je nezbytné pro splnění právní povinnosti, která se na správce vztahuje. Byť je aplikovatelné policejní právo věcí ve výlučné působnosti členských států, existují pravděpodobně v každém členském státě obecná pravidla upravující předávání důkazů donucovacím orgánům. GDPR upravuje zpracování předání dat správcem. Pokud vnitrostátní legislativa vyžaduje po správci, aby spolupracoval s donucovacími složkami (např. při vyšetřování), je právním důvodem pro předání údajů právní povinnost podle článku 6 (1) (c).

57. Omezení účelu v článku 6 (4) je často bezproblémové, neboť zpřístupnění je výslovně věcí práva členských zemí. Úvahy o zvláštních požadavcích pro změnu účelu ve smyslu písm. a - e nejsou proto nutné.

> Příklad: Majitel obchodu má kameru u vchodu. Ta zaznamená osobu kradoucí peněženku jiné osobě. Policie požádá správce o vydání záznamu za účelem jejího vyšetřování. V tomto případě uplatní správce právní důvod podle článku 6 (1) (c) (právní povinnost) v kombinaci s příslušným vnitrostátním právem upravujícím přenos zpracování.
>
> Příklad: V obchodě je z bezpečnostních důvodů umístěna kamera. Majitel obchodu se domnívá, že zaznamenal něco podezřelého u svého vchodu a rozhodne se postoupit materiál policii (aniž by měl informaci, že ve věci probíhá nějaké relevantní vyšetřování). V tomto případě musí majitel posoudit, zda jsou, ve většině případů, splněny podmínky článku 6 (1) (f).

58.

59. Zpracování osobních údajů samotnými donucovacími orgány samotnými nespadá pod GDPR (viz článek 2 (2) (d)), ale podléhá směrnici o vymáhání práva (EU2016/680).

5 ZPRACOVÁNÍ ZVLÁŠTNÍCH KATEGORIÍ ÚDAJŮ

60. Kamerové systémy obvykle shromažďují masivní množství osobních údajů, která mohou odhalit informace vysoce osobní povahy, dokonce i zvláštní kategorie údajů. Původně zcela nepodstatné údaje shromážděné prostřednictvím videa mohou být použity k odvození dalších informací pro dosažení jiného účelu (např. zmapování zvyků jednotlivce). Videosledování však není vždy považováno za systém zpracovávající zvláštní kategorie osobních údajů.

> Příklad: Kamerový záznam zobrazující subjekt údajů, který nosí brýle nebo užívá invalidní vozík, není *per se* považován za zvláštní kategorii osobních údajů.

61.

62. Pokud se však videozáznam zpracovává za účelem odvození zvláštních kategorií údajů, použije se článek 9.

> Příklad: Politické názory by například mohly být odvozeny z obrázků zobrazujících identifikovatelný subjekt údajů při účasti na určité akci, účasti na stávce apod. Takový případ by spadal pod článek 9.
>
> Příklad: Kamerové sledování v nemocnici instalované kvůli sledování zdravotního stavu pacientů bude považováno za zpracování zvláštních kategorií osobních údajů (Článek 9).

63.

64. Obecně platí zásada, že při zavádění kamerového systému by měla být pečlivě zvážena zásada minimalizace údajů. Proto i v případech, kdy se neuplatní článek 9 (1), by správce vždy měl usilovat o minimalizaci rizika zachycení záznamu odhalujícího další citlivé údaje (mimo rozsah článku 9) bez ohledu na účel.

> Příklad: Videozáznam zachycující kostel nespadá sám o sobě pod článek 9. Nicméně, správce by měl při posuzování zájmů subjektu údajů věc obzvláště pečlivě zvážit podle článku 6 (1) (f) a vzít v úvahu povahu dat a riziko záznamu jiných citlivých údajů (mimo rozsah článku 9).

65.

66. Pokud se pro zpracování zvláštních kategorií údajů používá systém kamerového dohledu, musí správce identifikovat jak výjimku pro zpracování zvláštních kategorií údajů podle článku 9 (tj. výjimku z obecného pravidla, že by zvláštní kategorie dat neměly být zpracovávány), tak stanovit právní důvod podle článku 6.

67. Například článek 9 (2) (c) (zpracování nutné k ochraně životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas) by – teoreticky a výjimečně – mohl být použit, ale správce by musel odůvodnit, že je to naprosto nezbytné k ochraně životně důležitých zájmů osoby, a prokázat, že tato osoba *„není fyzicky nebo právně způsobilá udělit souhlas“*. Správce navíc nebude moci použít systém z jakéhokoliv jiného důvodu.

> Příklad: Nemocnice sleduje pacienta ze zdravotních důvodů. Dotčený subjekt údajů byl přivezen do nemocnice záchrankou v bezvědomí. V tomto případě by mohl být použit článek 9 (2) (c).

68.

69. Je důležité poznamenat, že výjimky uvedené v článku 9 nebudou pravděpodobně použitelné k odůvodnění zpracování zvláštních kategorií dat prostřednictvím videosledování. Přesněji, správci zpracovávající taková data v souvislosti s videosledováním se nemohou spoléhat na článek 9 (2) (e), který umožňuje zpracování vztahující

se k osobním údajům zjevně zveřejněným subjektem údajů. Jen samotný fakt vstupu do záběru kamery neznamená, že subjekt údajů hodlá zveřejnit zvláštní kateorie údajů jež se ho týkají.

70. Zpracování zvláštních kategorií údajů navíc vyžaduje zvýšenou a neustálou pozornost vůči určitým povinnostem, například vysokou úroveň zabezpečení a provedení posouzení vlivu na ochanu osobních údajů, pokud je to nezbytné.

> Příklad: Zaměstnavatel nesmí používat záznamy z kamer zachycujících demonstraci, aby identifikoval stávkující.

71.

5.1 Obecné úvahy při zpracování biometrických dat

72. Použití biometrických údajů, a zvláště metody rozpoznávání obličeje, vyvolává zvýšené riziko pro práva subjektů údajů. Je zásadní, aby se využití takových technologií uskutečnilo při náležitém dodržování zásad zákonnosti, nezbytnosti, proporcionality a minimalizace údajů podle GDPR. I když nasazení takových technologií může být vnímáno jako obzvlášť efektivní, správci by měli v první řadě posoudit vliv na základní práva a svobody a zvážit použití méně rušivých prostředků k dosažení legitimního účelu zpracování.

73. Aby bylo data možné považovat za biometrická data definovaná v GDPR, musí zpracování hrubých dat zahrnovat měření určitých vlastností, jimiž jsou vlastnosti tělesné, fyziologické nebo znaky chování určité osoby. Vzhledem k tomu, že biometrická data jsou výsledkem těchto měření, stanoví GDPR v článku 4 (14), že jde o osobní údaje *„z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování“*. Videozáznam jednotlivce však nemůže být sám o sobě považován za biometrický údaj podle článku 9, nebyl-li specificky technicky zpracován za účelem přispět k identifikaci jednotlivce. [16]

74. Aby se jednalo o zpracování zvláštních kategorií osobních údajů (článek 9), požaduje se, aby biometrické údaje byly zpracovány „za účelem jedinečné identifikace fyzické osoby“.

75. Lze shrnout, že z hlediska článků 4 (14) a 9, musí být zvážena tři kritéria:

- **Povaha dat:** data týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby,
- **Prostředky a způsoby zpracování**: data „vyplývající z konkrétního technického zpracování“,
- **Účel zpracování:** data musí být použita za účelem jedinečné identifikace fyzické osoby.

76. Použití videosledování včetně funkce biometrického rozpoznávání instalovaného soukromým subjektem pro jeho vlastní účely (např. marketing, statistika nebo dokonce bezpečnost) bude ve většině případů vyžadovat

[16] Recitál 51 tuto analýzu podporuje, když uvádí, že *„zpracování fotografií by nemělo být systematicky považováno za zpracování zvláštních kategorií osobních údajů, neboť na fotografie se definice biometrických údajů vztahuje pouze v případech, kdy jsou zpracovávány zvláštními technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby“*.

výslovný souhlas všech subjektů údajů (Článek 9 (2) (a)), i když by mohla by být aplikovatelná i některá další vhodná výjimka podle článku 9.

Příklad: Pro zlepšení svých služeb nahradila soukromá společnost přepážky pro cestující na letišti (odbavení zavazadel, nástup) systémy kamerového sledování, které používají techniky rozpoznávání obličeje k ověřování totožnosti cestujících, kteří dali souhlas s takovým postupem. Protože toto zpracování spadá pod článek 9, musí se cestující, kteří dali předem výslovný a informovaný souhlas, zaregistrovat například přes automatický terminál za účelem vytvoření a uložení šablony jejich obličeje, která je spojena s jejich palubní vstupenkou a identitou. Odbavovací terminály s rozpoznáváním obličeje musí být zřetelně oddělené, např. systém musí být konstrukčně nainstalován tak, aby nebylo možno shromažďovat biometrické šablony osob, které souhlas neudělily. Zařízení s biometrickým systémem budou tedy využívat pouze cestující, kteří předem dali souhlas a zaregistrovali se.

Příklad: Správce řídí přístup do budovy pomocí metody rozpoznávání obličeje. Lidé mohou tento způsob vstupu používat pouze, pokud předem udělili výslovný a informovaný souhlas (podle článku 9 (2) (a)). Nicméně, aby se zajistilo, že nikdo nebude snímán bez předchozího souhlasu, měla by metoda rozpoznávání obličeje spuštěna samotným subjektem údajů, například stisknutím tlačítka. Pro zajištění zákonnosti zpracování musí správce vždy nabídnout alternativní způsob vstupu bez biometrického zpracování jako je např. visačka nebo klíče.

77.

78. V případech, kde jsou generovány biometrické šablony, musí správci zajistit, aby poté jakmile je získán souhlasný nebo nesouhlasný výsledek o shodě nebo naopak neshodě, byly všechny průběžné šablony vytvořené během procesu (na základě výslovného a informovaného souhlasu subjektu údajů) za účelem porovnání s těmi, které byly zaevidovány při registraci subjektu údajů, okamžitě a bezpečně smazány. Šablony vytvořené pro registraci by měly být uchovávány pouze pro uskutečnění účelu zpracování a neměly by být uchovávány nebo archivovány.

79. Nicméně, pokud je účelem zpracování například rozlišení kategorií lidí, nikoliv jedinečná identifikace jednotlivců, takové zpracování nespadá pod článek 9.

Příklad: Majitel obchodu by chtěl přizpůsobit svou reklamu pohlaví a věku zákazníků, přičemž tyto informace chce získat prostřednictvím videosledování. Pokud takový systém nevytváří biometrické šablony za účelem jedinečné identifikace osob, ale pouze zjišťuje typické fyzické chrarakteristiky a podle nich osoby klasifikuje, pak toto zpracování nespadá pod článek 9.

80.

81. Článek 9 se však použije, pokud správce ukládá biometrické údaje (většinou jako šablony vytvořené extrakcí klíčových vlastností ze surové formy biometrických dat (např. měření obličeje podle obrázku)) za účelem jedinečné identifikace osoby. Pokud chce správce znovu určit subjekt údajů vstupující do určitého nebo jiného prostoru (například za účelem šíření cílené reklamy), bude účelem jedinečná identifikace fyzické osoby, což by znamenalo, že taková operace od počátku spadá pod článek 9. To by mohl být případ, kdy správce uchovává vytvořené šablony za účelem umisťování další cílené reklamy na několika reklamních upoutávkáh v různých částech obchodu. Protože tento systém používá fyzické vlastnosti ke zjišťování konkrétních jednotlivců opětovně vstupujících do záběru kamery (typicky návštěvníci nákupního centra) a sleduje je, jedná se o metodu biometrické identifikace, neboť cílem je rozpoznání pomocí konkrétního technického zpracování.

Příklad: Majitel obchodu nainstaloval ve svém obchodě systém rozpoznávání obličeje, aby přizpůsobil svou reklamu jednotlivcům. Před použitím tohoto biometrického systému a zasláním přizpůsobené reklamy musí správce údajů získat výslovný a informovaný souhlas všech subjektů údajů. Systém by byl nezákonný, pokud by zachytil návštěvníky nebo kolemjdoucí, kteří nesouhlasili s vytvořením jejich biometrické šablony, i když by jejich šablona byla v nejkratší možné době vymazána. Tyto dočasné šablony představují biometrická data zpracovaná za účelem jedinečné identifikace osoby, která nemusí mít zájem dostávat cílenou reklamu.

82.

83. Evropský sbor pro ochranu osobních údajů (EDPB) poznamenává, že některé biometrické systémy jsou instalovány v nekontrolovaném prostředí[17], což znamená, že systém průběžně zaznamená tvář každého jednotlivce procházejícího před zorným polem kamery včetně osob, které neudělily souhlas s biometrickým zařízením, a tedy s vytvořením biometrických šablon. Tyto šablony jsou porovnávány se šablonami subjektů údajů, které předem souhlasily s registračním procesem (např. uživatel biometrického zařízení), aby správce zjistil, zda jde o osobu užívající biometrické zařízení nebo nikoliv. V tomto případě je systém často navržen jako diskriminační vůči jednotlivcům, neboť rozlišuje mezi těmi, kdo jsou a nejsou v databázi. Vzhledem k tomu, že účelem je jedinečná identifikace fyzických osob, je i nadále potřebná výjimka podle článku 9 (2) pro kohokoliv zachyceného kamerou.

Příklad: Hotel používá systém videosledování k automatickému upozornění recepčního, že přijela VIP osoba, jakmile systém rozpozná jeho obličej. Tyto VIP osoby udělily výslovný souhlas s použitím rozpoznávání obličeje předtím, než byly zaznamenány do databáze vytvořené pro tento účel. Tyto systémy zpracování biometrických dat by byly nezákonné, pokud by všichni další monitorovaní hosté (za účelem identifikace VIP osob) neudělili souhlas se zpracováním podle článku 9 (2) (a).

Příklad: Správce instaloval systém videosledování s rozpoznáváním obličeje u vchodu do koncertní síně, kterou provozuje. Správce musí zřídit zřetelně oddělené vchody; jeden s biometrickým systémem a další bez něho (kde se namísto použití biometrického systému například skenují vstupenky). Vchody vybavené biometrickým zařízením musí být instalovány a zpřístupněny způsobem, který zabrání snímání biometrických šablon diváků, kteří nedali svůj souhlas se zpracováním.

84.

85. Konečně, je-li požadován souhlas podle článku 9, nesmí správce podmiňovat přístup ke svým službám akceptací biometrického zpracování. Jinými slovy, zejména když se biometrické zpracování používá pro účel autentizace, správce musí nabídnout alternativní řešení nezahrnující biometrické zpracování – bez omezení nebo dodatečných nákladů pro subjekt údajů. Toto alternativní řešení je nutné také pro osoby, které nemohou používat biometrická zařízení z důvodu určitých omezení (nemožnost registrace nebo čtení biometrických dat, obtížné použití zařízení z důvodu postižení apod.). Také při nedostupnosti biometrického zařízení (např. špatná funkce zařízení) musí existovat záložní řešení, aby byla zajištěna kontinuita nabízené služby, omezená ovšem na výjimečná použití.

[17] Znamená to, že biometrické zařízení je umístěno v prostoru otevřeném veřejnosti a je schopno zachytit každého kolemjdoucího, na rozdíl od biometrických systémů v kontrolovaném prostředí, kde může být použito jen vůči osobám, které udělily souhlas.

5.2 Opatření navrhovaná k minimalizaci rizik při zpracování biometrických údajů

86. V souladu se zásadou minimalizace údajů musí správci zajistit, aby data extrahovaná z digitálního obrazu za účelem vytvoření šablony nebyla nadbytečná a obsahovala pouze informace požadované pro daný konkrétní účel, aby se vyloučilo jakékoli další možné zpracování. Měla by být uplatněna opatření zajišťující, že šablony nebudou přenášeny mezi různými biometrickými systémy.

87. Identifikace a autentizace/verifikace budou pravděpodobně vyžadovat uchovávání šablon pro pozdější srovnávání. Správce musí zvážit nejvhodnější umístění uchovávaných dat. V kontrolovaném prostředí (ohraničené chodby nebo kontroní body) mají být šablony uchovávány na individuálním zařízení v držení uživatele a pod jeko výhradní kontrolou (v chytrém telefonu bebo na ID kartě) nebo – pokud je to potřeba pro konkrétní účely a je to objektivně nutné – uchovávány v centralizované databázi v šifrované formě s klíčem/tajnou informací pouze v rukou osoby, která brání neoprávněnému přístupu k šabloně nebo místu uložení. Nemůže-li správce zabránit přístupu k šablonám, musí podniknout vhodné kroky k zajištění bezpečnosti uložených údajů. To může zahrnovat zašifrování šablony kryptografickým algoritmem.

88. Správce musí v každém případě učinit veškerá preventivní opatření k zachování dostupnosti, integrity a důvěrnosti zpracovaných dat. Za tímto účelem má správce zejména učinit následující opatření: oddělení dat během přenosu a ukládání, uložení biometrických šablon a surových dat nebo údajů o identitě v odlišných databázích, zašifrování biometrických dat zejména biometrických šablon, stanovení politiky pro šifrování a správu klíčů, zavedení organizačních a technických opatření pro odhalování podvodů, provázání kódu integrity s daty (například podpis nebo hash) a zákaz jakéhokoliv vnějšího přístupu k biometrickým údajům.

89. Správci kromě toho musí přikročit k výmazu surových dat (obrázky tváří, řečové signály, způsob chůze atd.) a zajistit účinnost tohoto výmazu. Jelikož biometrické šablony jsou odvozeny z takových dat, lze se domnívat, že vytváření databází by mohlo představovat stejnou, ne-li větší hrozbu (protože nemusí být vždy snadné přečíst biometrickou šablonu bez znalosti toho, jak byl její vznik programován, zatímco surová data jsou stavebním kamenem jakékoliv šablony). V případě, že bude správce potřebovat tato data uchovat, musí prozkoumat možnost uplatnění „*noise-additive*“ metody (podobné vodoznaku), která učiní vytvořenou šablonu neúčinnou. Správce také musí smazat biometrické údaje a šablony v případě neoprávněného přístupu do čtecího srovnávacího terminálu nebo úložného serveru a mazat veškerá data, která nejsou potřebná k dalšímu zpracování na konci životnosti biometrického zařízení.

6 PRÁVA SUBJEKTU ÚDAJŮ

90. Vzhledem k povaze zpracování údajů při použití kamerových systémů vyžadují některá práva subjektu údajů stanovená v GDPR podrobnější objasnění. Tato kapitola však není vyčerpávající, na zpracování osobních údajů prostřednictvím kamer lze použít veškerá práva podle GDPR.

6.1 Právo přístupu

91. Subjekt údajů má právo získat od správce potvrzení, zda zpracovává nebo nezpracovává jeho osobní data. Z hlediska kamerového sledování to znamená, že pokud data nejsou uchovávána nebo předávána jiným způsobem než jednorázově v okamžiku záběru, potom jakmile uplyne okamžik jednorázového monitorování, by správce mohl pouze sdělit, že žádné osobní údaje nejsou nadále zpracovávány (kromě obecných informačních povinností podle článku 13, viz *kapitola 7 – Transparentnost a informační povinnost*). Jsou-li však data v době žádosti stále zpracovávána (tj. pokud jsou údaje uloženy nebo průběžně zpracovávány jakýmkoliv jiným způsobem), subjekt údajů by měl obdržet přístup k údajům a informaci v souladu s článkem 15.

92. Existuje však řada omezení, která se mohou v některých případech vztahovat na právo přístupu.

- Článek 15 (4), nepříznivé dotčení práv jiných osob

93. Vzhledem k tomu, že ve stejné videosekvenci v rámci kamerového dohledu může být zaznamenáno více subjektů údajů, bude screening představovat dodatečné zpracování osobních údajů ostatních subjektů údajů. Pokud subjekt údajů bude chtít získat kopii zpracovávaných osobních údajů (článek 15 (3), může se to nepříznivě dotknout práv a svobod jiných subjektů údajů zaznamenaných v kopii materiálu. Aby se tomu zabránilo, správce by měl zvážit, zda vzhledem k narušující povaze videozáznamu by v některých případech neměl odepřít předání záznamu, na kterém by bylo možno identifikovat jiné subjekty údajů. Ochrana práv třetích stran by však neměla být použita jako výmluva k zamezení oprávněných nároků jednotlivců. Namísto toho by měl správce použít taková technická opatření, která mu umožní vyhovět žádosti o přístup splnit (například, technologie editace obrazu jako maskování nebo kódování).

- Ćlánek 11 (2), správce není schopen identifikovat subjekt údajů

94. Pokud videozáznam neumožňuje vyhledávat osobní údaje, (tj. správce by pravděpodobně musel procházet velkým množstvím uloženého materiálu, aby našel dotčený subjekt údajů), správce nemusí být schopen subjekt údajů identifikovat.

95. Z těchto důvodů by subjekt údajů měl (kromě vlastní identifikace spočívající v identifikaci prostřednictvím dokumentu nebo osobně) ve své žádosti vůči správci upřesnit, kdy – v rozumném časovém rozsahu proporcionálnímu vzhledem k množství zaznamenaných subjektů údajů – vstoupil do monitorovaného prostoru. Správce by měl subjektu údajů předem oznámit jaké informace jsou potřebné, aby vyhověl žádosti. Pokud je správce schopen doložit, že pro něj není možné subjekt údajů iodentifikovat, správce musí odpovídajícím způsobem informovat subjekt údajů.

> Příklad: Požaduje-li subjekt údajů kopii svých osobních údajů zpracovávaných prostřednictvím videosystému při vstupu do obchodního centra se 30 000 návštěvníky denně, měl by subjekt údajů upřesnit, kdy procházel sledovaným prostorem s přesností přibližně dvouhodinového časového intervalu. Pokud správce stále zpracovává materiál, měl by poskytnout kopii videozáznamu. Pokud lze v daném materiálu identifikovat i jiné subjekty údajů, měla by být tato část záznamu anonymizována před tím, než je kopie předána subjektu údajů, který podal žádost (například rozostřením kopie nebo jejích částí).
>
> Příklad: Pokud správce automaticky maže veškeré záznamy například do dvou dnů, může subjekt údajů získat přístup jen k této informaci [neboť materiál byl smazán], pokud jeho žádost byla podána správci po těchto dvou dnech.

96.

- Článek 12, nepřiměřené žádosti

96. V případě nepřiměřených nebo zjevně neopodstatněných žádostí subjektů údajů může správce buď účtovat přiměřený poplatek v souladu s článkem 12 (5) (a) nebo odmítnout žádost (článek 12 (5) (b). Správce musí být schopen doložit, že žádost byla nepřiměřená nebo nepodložená.

6.2Právo na výmaz a právo vznést námitku

6.2.1 Právo na výmaz (Právo být zapomenut)

98. Pokud správce pokračuje ve zpracování osobních údajů nad rámec sledování v reálném čase (např. uložení), může subjekt údajů požadovat výmaz osobních údajů podle článku 17.

99. Správce je povinen na vyžádání smazat osobní údaje bez zbytečného odkladu, nastane-li některá z okolností uvedených v článku 17 (1) (a neuplatní se žádná z výjimek vyjmenovaných v článku 17 (3)). To zahrnuje povinnost vymazat osobní údaje, pokud již nejsou potřebné pro účely, pro které byly původně uloženy nebo pokud je zpracování nezákonné (viz také kapitola 8 o době uložení a povinnosti výmazu). Kromě toho by v závislosti na právním dvodu zpracování měly být osobní údaje vymazány v následujících případech:

- *v případě souhlasu* vždy, když je souhlas odvolán (a pro zpracování neexistuje žádný jiný právní důvod)
- v případě oprávněného zájmu:
    - vždy když subjekt údajů uplatní právo vznést námitku (viz *kapitola 6.2.2*) a neexistuje žádný závažný naléhavý právní důvod pro zpracování, nebo
    - v případě přímého marketingu (včetně profilování) vždy, když subjekt údajů vznese námitku vůči zpracování.

100. Pokud správce zveřejnil videozáznam (např. vysílání nebo streamování online), je třeba učinit přiměřené kroky k informování ostatních správců (kteří v té době zpracovávají dotčené osobní údaje) o žádosti podle článku 17 (2). Přiměřené kroky by měly zahrnovat technická opatření zohledňující dostupnou technologii a náklady na provedení. Správce by měl v nejširším možném rozsahu vyrozumět – při výmazu osobních údajů – každého, komu byly dříve osobní údaje zpřístupněny, a to v souladu s článkem 19.

101. Kromě povinnosti správce vymazat osobní údaje na žádost subjektu údajů, je správce povinen podle obecných zásad GDPR omezit uložení uchovávaných osobních údajů (viz *kapitola 8)*.

102. V případě videosledování stojí za zmínku, že například rozmazání obrázku s nemožností retroaktivity, tedy obnovení osobních údajů, které snímek původně obsahoval, je považováno za výmaz ve smyslu GDPR.

> Příklad: Obchod se smíšeným zbožím má potíže s vandalismem, zejména pokud jde o venkovní prostor, a používá tedy videodohled upevněný na zdi vně vchodu. Kolemjdoucí požaduje výmaz jeho zaznamenaných osobních údajů. Správce je povinen odpovědět na žádost bez zbytečného odkladu, nejpozději do jednoho měsíce. Vzhledem k tomu, že předmětné záznamy již nesplňují účel, pro který byly původně uloženy (nedošlo k žádnému vandalismu v době, kdy prošel subjekt údajů), neexistuje v době žádosti žádný oprávněný zájem na uložení dat, který by převažoval nad zájmem subjektů údajů. Správce tedy musí osobní údaje vymazat.

103.

6.2.2 Právo vznést námitku

104. V případě videosledování založeného na *oprávněném zájmu* (článek 6 (1) (f)) nebo na nezbytnosti splnit úkol ve *veřejném zájmu* (Článek 6 (1) (e)) má subjekt údajů – kdykoli – vznést námitku vůči zpracování podle článku 21/2 na základě své konkrétní situace. Pokud správce neprokáže přesvědčivý legitimní důvod převažující nad právy a zájmy subjektu údajů, musí být zastaveno zpracování dat osoby, která vznesla námitku. Správce by měl být povinen odpovědět na žádosti od subjektu údajů bez zbytečného odkladu, nejpozději do jednoho měsíce.

105. V souvislosti s videosledováním by mohla být vznesena námitka buď před vstupem do monitorovaného prostoru, během pobytu v něm nebo po jeho opuštění. V praxi to znamená, že pokud správce nemá přesvědčivé legitimní důvody pro sledování prostoru, v němž by mohla být identifikována fyzická osoba, je zpracování zíkonné pouze, pokud:

(1) správce je schopen okamžitě na požádání zastavit zpracovávání osobních údajů kamerou, nebo

(2) monitorovaná oblast je do takové míry omezena, že správce může zajistit souhlas od subjektu údajů ještě před vstupem do této zóny, a přitom se nejedná o oblast, do které má subjekt údajů jako občan právo na přístup.

106. Při použití kamerového systému pro účely přímého marketingu má subjekt údajů právo vznést námitky vůči zpracování na základě volného uvážení, neboť právo vznést námitku je v této souvislosi absolutní (Článek 21 (2) a (3)).

Příklad: Firma má problémy s narušováním bezpečnosti u vchodu pro veřejnost a používá videodohled na základě oprávněného zájmu za účelem zachytit nezákonně vstupující osoby. Návštěvník vznese námitku vůči zpracování svých osobních údajů prostřednictvím videosystému z důvodů týkajících se jeho konkrétní situace. Firma však v tomto případě jeho žádost odmítne s vysvětlením, že uložené záznamy jsou potřebné kvůli probíhajícímu internímu vyšetřování, a tudíž má přesvědčivý legitimní důvod pokračovat ve zpracování sporných osobních údajů.

107.

7 TRANSPARENTNOST A INFORMAČNÍ POVINNOST[18]

108. Evropské právo na ochranu dat je dlouhodobě založeno na požadavku, že subjekty údajů by si měly být vědomy, že jsou objektem videosledování. Měly by být podrobně informovány ohledně míst, která jsou monitorovány.[19] GDPR stanoví obecné podmínky týkající se transparentnosti a informačních povinností v článku 12 a násl. Další podrobnosti stanoví dokument Pracovní skupiny WP29 „Pokyny k transparentnosti podle nařízení 2016/679 (WP260)", které byly přijaty EDPB dne 25. května 2018. Článek 13 GDPR je v souladu s odstavcem 26 dokumentu WP260 aplikovatelný, pokud jsou osobní údaje shromažďovány „od subjektu údajů sledováním (např. pomocí automatizovaných zařízení pro sběr dat nebo softwaru na zaznamenávání dat jako jsou kamery)".

109. Vzhledem k množství informací, které mají být subjektu údajů poskytnuty, mohou správci zvolit vícevrstevnatý přístup v případech, kdy se rozhodnou využít kombinaci metod k zajištění transparentnosti (WP260 odst. 35; WP89 str. 22). Pokud jde o videosledování, nejdůležitější informace by měly být uvedeny na samotném varovném oznámení (první vrstva), zatímco další povinné podrobnosti lze sdělit jinými prostředky (druhá vrstva).

[18] Zde mohou platit zvláštní požadavky vnitrostátní legislativy.

[19] Pracovní skupina WP29, Stanovisko 4/2004 ke zpracování osobních údajů prostředky videosledování (WP89).

19

7.1 První vrstva informace (varovné oznámení)

110. První vrstva se primárně týká způsobu, jakým se správce poprvé dostává do kontaktu se subjektem údajů. V této fázi mohou správci použít varovné oznámení znázorňující podstatné informace. Zveřejněné informace mohou být poskytnuty v kombinaci s ikonou tak, aby by byl podán smysluplný přehled zamýšleného zpracování snadno viditelným, srozumitelným a čitelným způsobem (článek 12 (7). Formát informace by měl být přizpůsoben konkrétnímu umístění (WP89 str. 22).

7.1.1 Umístění varovného oznámení

111. Informace by měly být umístěny v přiměřené vzdálenosti od sledovaných prostor (WP 89 str. 22), a to takovým způsobem, aby subjekt údajů snadno rozeznal okolnosti sledování před stupem do monitorovaného prostoru (přibližně ve výši očí). Není nutné specifikovat přesné umístění sledovacího zařízení, pokud nejsou pochyby o tom, které plochy jsou předmětem monitorování, a je jednoznačně objasněn kontext sledování (WP 89 str. 22). Subjekt údajů musí být schopen odhadnout, který prostor je zabírán kamerou, aby se mohl vyhnout sledování nebo v případě nutnosti přizpůsobil své chování.

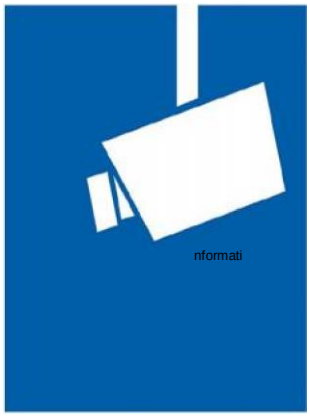
7.1.2 Obsah informace v první vrstvě

112. Informace v první vrstvě (varovné oznámení) by obecně měly sdělovat nejdůležitější informace, např. údaje ohledně účelu(ů) zpracování, totožnosti správce a existenci práv subjektu údajů společně s informací o nejzávažnějších dopadech zpracování.[20] To může například zahrnovat oprávněné zájmy sledované správcem (nebo třetí stranou) a kontaktní údaje pověřence pro ochranu osobních údajů (pokud je jmenován). Také se musí odkazovat na podrobnější informace ve druhé vrstvě a uvést, jak se k nim dostat.

113. Oznámení by také mělo obsahovat veškeré informace o zpracování, které by pro subjekt údajů mohly být překvapivé (WP 260 odst. 38). Mohlo by se například jednat o informace o přenosu třetím stranám, zvláště pokud sídlí mimo EU, a ohledně doby uchovávání. Pokud tato informace není uvedena, subjekt údajů by měl důvěřovat, že se jedná pouze o živé monitorování (bez jakéhokoliv záznamu dat nebo jejich přenosu třetím stranám).

[20] Viz WP 260 odst. 38.

Příklad:



Videosledování

Identita správce, případně jeho zástupce.

Kontaktní údaje pověřence pro ochranu osobních údajů, pokud je jmenován:

Účel, pro který je zpracování osobních údajů zamýšleno a právní důvod zpracování:

Další informace jsou dostupné:
- - Sdělení o ochraně osobních údajů
- Informace na recepci/v zákaznickém centru
- informace na internetu (odkaz)

Práva subjektu údajů: Jako subjekt údajů máte několik práv vůči správci, konkrétně právo na přístup či právo na výmaz.

K podrobnostem o videosledování včetně vašich práv viz plná informace správce, odkazy ve sloupci nalevo.

114.

7.2 Druhá vrstva informací

115. Druhá vrstva Informací musí být také dostupná na místě snadno přístupném pro subjekt údajů, například jako kompletní informační list dostupný v nějakém cetrálním místě (např. informační přepážka, recepce nebo pokladna) nebo zveřejněný na snadno přístupném letáku. Jak bylo uvedeno výše, první vrstva informace musí zřetelně odkazovat na druhou vrstvu. Navíc je nejvhodnější, pokud první vrstva odkazuje na nějaký digitální zdroj druhé vrstvy informace (např. QR kód nebo webová adresa). Informace by ovšem měla být snadno dostupná i v jiné než digitální formě. V každém případě musí být možný přístup k informacím druhé vrstvy i bez vstupu do monitorované oblasti. Toho lze dosáhnout například odkazem na online link nebo nějakým jiným vhodným způsobem, např. uvedením telefonního čísla. Je nutné uvést i všechny další informace, které jsou podle článku 13 povinné.

116. Vedle těchto možností a také se záměrem jejich větší efektivnosti podporuje EDPB využívání technologických prostředků k poskytování informací subjektům údajů. To může zahrnovat například geolokační kamery a zahrnutí informací do mapových aplikací nebo do webových stránek, aby tak ednotlivci mohli jednak snadno identifikovat a specifikovat videozdroje související s výkonem jejich práv, a dále aby získali podrobnější informace o operaci zpracování.

Příklad: Majitel monitoruje svůj obchod. K dosažení souladu s článkem 13 je postačující umístit na snadno viditelné místo u vstupu do obchodu varovné oznámení, které bude obsahovat informace první vrstvy. Kromě toho musí poskytnout u pokladny nebo jiném centrálním a snadno dostupném místě v obchodě informační list obsahující informace druhé vrstvy.

117.

8 DOBA ULOŽENÍ A POVINNOST VÝMAZU

118. Osobní údaje nesmí být uchovávány déle, než je nezbytné pro účel, pro který jsou zpracovávány (článek 5 (1) (c) a (e)). V některých členských státech mohou existovat zvláštní ustanovení ohledně doby uchovávání ve vztahu k videosledování podle článku 6 (2).

119. V krátkých časových intervalech by mělo být kontrolováno, zda je nezbytné uchovávat osobní údaje nebo ne. Obecně je častým legitimním účelem videosledování ochrana majetku nebo uchování důkazů. Škody, které mohou vzniknout, mohou být obvykle odhaleny během jednoho nebo dvou dnů. S přihlédnutím k zásadám podle článku 5 (1) (c) a (e), zejména k minimalizaci údajů a omezení uložení, by osobní údaje měly být ve většině případů (např. za účelem odhalení vandalismu) vymazány během několika málo dnů, ideálně automaticky. Čím déle je nastavena doba uchovávání (zvlášť za hranici 72 hodin), tím musí být předložena rozsáhlejší argumentace pro legitimitu účelu a nezbytnost uchování. Pokud správce používá videosledování nejen k monitorování svých prostor, ale také má v úmyslu tato data uchovávat, musí zajistit, aby uchovávaná data byla skutečně nezbytná k dosažení účelu. Doba uchování musí být jasně definována a individuálně nastavena pro každý jednotlivý účel. Je odpovědností správce definovat dobu uchování v souladu se zásadami nezbytnosti a proporcionality a prokázat soulad s ustanoveními GDPR.

> Příklad: Majitel malého obchodu si obvykle všimne vandalismu ten stejný den, kdy k němu dojde. Z toho plyne, že obvyklá doba uchovávání záznamu 24 hodin je dostatečná. Víkend nebo dovolená by však mohli být důvodem pro delší dobu uchování. Také v případě, že dojde ke škodě, může být potřebné uchovávat videozáznam delší dobu kvůli případné žalobě na pachatele.

120.

9 TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ

121. Jak je uvedeno v článku 32 (1), zpracování osobních údajů během videosledování musí být nejenom zákonné, ale správci a zpracovatelé je také musí přiměřeně zabezpečit. Zavedená **organizační a technická opatření** musí být **přiměřená rizikům pro práva a svobody fyzických osob**, které hrozí jako následek náhodného nebo nezákonného zničení, ztráty, pozměnění, neoprávněného zpřístupnění nebo přístupu k datům z videosystému. Podle článku 24 a 25 musí správci zavést technická a organizační opatření také za účelem zabezpečení všech zásad ochrany dat během zpracování a stanovit prostředky pro výkon práv subjektu údajů definované v článcích 15 – 22. Správci údajů by měli vytvořit interní rámec a politiku, které zajistí tuto implementaci, jak v době stanovení prostředků zpracování, tak během samotného zpracování, včetně vypracování posouzení vlivu na ochranu osobních údajů, pokud je potřebné.

9.1Přehled systémů kamerového dohledu

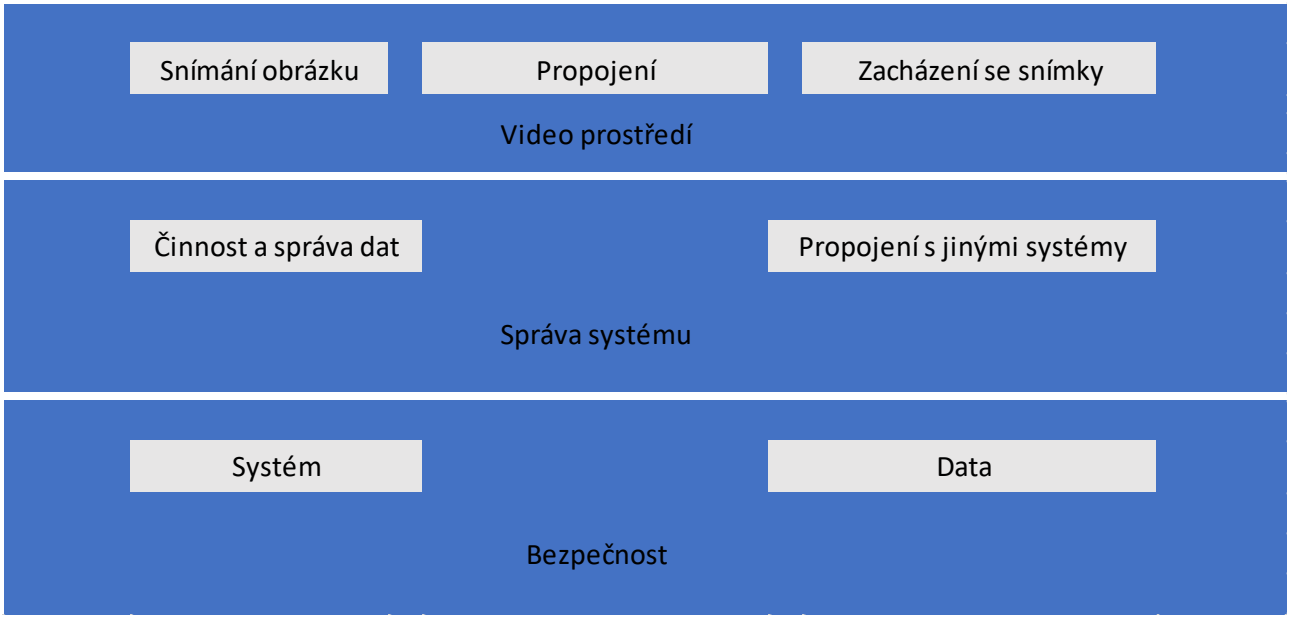
Systém videosledování[21] sestává z analogových nebo digitálních zařízení, případně ze softwaru pro potřeby snímání scénických snímků, jejich zpracování a zobrazení operátorovi. Jeho komponenty jsou rozděleny do následujících kategorií:

- Videoprostředí: snímání obrazu, propojení a nakládání se snímky
    - účelem snímání snímků je vytvoření obrazu skutečného světa v takovém formátu, který lze použít dalšími částmi systému

[21] GDPR nenabízí definici, technický popis lze nalézt například v EN 62676-1-1:2014 Video surveillance systems for use in security applications – Part 1-1: Video system requirements.

- propojení charakterizuje jakýkoliv přenos dat v rámci videoprostředí, tj. spojení a komunikaci. Příkladem spojení jsou kabely, digitální sítě a bezdrátové přenosy. Komunikace znamená všechny obrazové a řídící datové signály, které mohou být digitální nebo analogové
- nakládání se snímky zahrnuje analýzu, uchovávání a prezentaci jednotlivého snímku nebo jejich sekvence

- Z pohledu systémového řízení má systém videosledování následující logické funkce:
  - správa dat a činností, které zahrnují plnění operátorových příkazů a systémem generovaných činností (poplachové postupy, pohotovost pro operátory)
  - rozhraní vůči jiným systémům může zahrnovat spojení s dalšími zabezpečovacími systémy (kontrola přístupu, požární alarm) i se systémy, jejichž účelem není bezpečnost (systémy správy budov, automatické rozpoznávání poznávacích značek)
- Zabezpečení videosystému spočívá v důvěrnosti, integritě a dostupnosti systému
  - systémová bezpečnost zahrnuje fyzické zabezpečení všech systémových součástí a ovládání přístupu k videosystému
  - bezpečnost dat zahrnuje prevenci ztráty dat a manipulace s nimi



122.

Obrázek 1 – systém videosledování

9.2 Záměrná a standardní ochrana osobních údajů

123. Jak je uvedeno v článku 25, správci musí zavést vhodná technická a organizační opatření ochrany dat, v době, jakmile plánují videosledování, ještě před započetím sběru a zpracování videozáznamů. Tyto zásady zdůrazňují potřebu zabudovaných technologií chránících soukromí, výchozí nastavení minimalizující zpracování dat a poskytnutí nezbytných nástrojů, které umožňují nejvyšší možnou ochranu osobních údajů.[22]

[22] Stanovisko 168 k „Budoucnost soukromí“, společná práce Pracovní skupiny WP29 a Pracovní skupiny pro policii a spravedlnost v rámci konzultace Evropské komise k právnímu rámci základního práva na ochranu

124. Správci by měli zabudovat záruky ochrany dat a soukromí nejenom do navržených specifikací dané technologie, ale také do organizačních postupů. Pokud jde o organizační postupy, správce by měl přijmout vhodný rámec řízení a stanovit a prosazovat politiky a postupy týkající se videosledování. Z technického hlediska by systém specifikace a projektování měl zahrnovat požadavky na zpracování osobních údajů v souladu se zásadami stanovenými v článku 5 (zákonnost zpracování, účelové omezení, minimalizace dat od návrhu, a to standardně ve smyslu článku 25 (2), integrita a důvěrnost, odpovědnost atd.). Pokud správce plánuje pořízení komerčního videosystému, musí tyto požadavky uvést v nákupní specifikaci. Správce musí zajistit soulad s těmito požadavky a uplatnit je u všech komponent systému a u všech jím zpracovávaných údajů, a to po celou dobu životního cyklu.

9.3 Konkrétní příklady relevantních opatření

125. Většina opatření, která mohou být použita k zabezpečení při videosledování, zejména v případě použití digitálního vybavení a softwaru, se nebude lišit od opatřeních používaných u jiných IT systémů. Nicméně, bez ohledu na zvolené řešení, musí správce adekvátně chránit všechny komponenty videosystému a data ve všech fázích, tj., během ukládání (data v klidu), přenosu (data v tranzitu) a zpracování (používaná data). K tomu je nezbytné, aby správci a zpracovatelé kombinovali organizační a technická opatření.

126. Při výběru technických řešení by měl správce zohlednit technologie přátelské vůči soukromí také proto, že posilují bezpečnost. Příkladem takových technologií jsou systémy umožňující maskování nebo kódování oblastí, které nejsou relevantní pro sledování, nebo vystříhání obrázků třetích osob před poskytnutím videozáznamu subjektům údajů.[23] Na druhé straně by zvolená řešení neměla mít funkce, které nejsou potřebné (např. neomezený pohyb kamer, schopnost zoomování, rádiový přenos, analýza a zvukový záznam). Nepotřebné funkce, byť dostupné, musí být deaktivovány.

127. K tomuto tématu existuje mnoho dostupné literatury včetné mezinárodních standardů a technických specifikací ohledně fyzického zabezpečení multimediálních systémů[24] a bezpečnosti IT systémů obecně[25]. Proto tato část poskytuje pouze celkový přehled tohoto tématu.

9.3.1 Organizační opatření

128. Pokud ponecháme stranou případné posouzení vlivu na ochranu osobních údajů (DPIA, viz kapitola 10), správci by ve vztahu k videosledování měli zvážit při tvorbě svých politik a postupů následující otázky:

- Kdo je zodpovědný za správu a provoz systému videosledování
- Účel a rozsah projektu videosledování

---

osobních údajů (přijato 1. prosince 2009), https://ec.europa.eu/justice/Article29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

[23] Použití takových technologií může být dokonce v některých případech povinné pro dosažení souladu s článkem 5 (1) (c). Každopádně mohou sloužit jako příklady dobré praxe.

[24] IEC TS 62045 — Multimedia security - Guideline for privacy protection of equipment and systems in and out of use

[25] ISO/IEC 27000 — Information security management systems series

[23] Použití takových technologií může být dokonce v některých případech povinné pro dosažení souladu s článkem 5 (1) (c). Každopádně mohou sloužit jako příklady dobré praxe.

[24] IEC TS 62045 — Multimedia security - Guideline for privacy protection of equipment and systems in and out of use

[25] ISO/IEC 27000 — Information security management systems series

[24] IEC TS 62045 — Multimedia security - Guideline for privacy protection of equipment and systems in and out of use.

[25] ISO/IEC 27000 – Information security management systems series

- Přípustné a zakázané použití (kde a kdy je videosledování dovoleno a kdy nikoliv; např. použití skrytých kamer a audiozařízení jako doplňku videonahrávky)[26]
- Opatření týkající se transparentnosti, jak je zmíněno v kapitole 7 (Transparentnost a informační povinnosti)
- Jakým způsobem je video nahráváno a v jaké délce trvání včetně archivace videozáznamů týkajících se bezpečnostních incidentů
- Kdo musí absolvovat příslušné školení a kdy
- Kdo má přístup k videozáznamům a za jakým účelem
- Provozní postupy (např. kým a odkud je monitorováno videosledování, co dělat v případě porušení ochrany dat)
- Jaké postupy musí dodržovat externí strany, pokud žádají o videozáznamy, a jaké jsou postupy pro odmítnutí nebo vyhovění takové žádosti
- Postupy při nákupu videozařízení, instalaci a údržbě
- Postupy v případě incidentu a nápravné postupy.

9.3.2 Technická opatření

129. **Systemová bezpečnost** znamená **fyzické zabezpečení** všech součástí systému a integritu systému, tj. **ochranu a odolnost vůči úmyslnému a neúmyslnému zásahu do běžných operací** a **kontrolu přístupu**. Zabezpečení dat znamená **důvěrnost** (data jsou přístupná pouze těm, kterým byl udělen přístup), **integritu (**prevenci proti ztrátě dat nebo manipulaci s nimi) a **dostupnost** (k datům je přístup, pokud je to potřebné).

130. **Fyzická bezpečnost** je důležitou součástí ochrany dat a první linií obrany, protože chrání systém videosledování proti krádeži, vandalismu, přírodními katastrofami, katastrofami způsobenými člověkem a náhodným poškozením (např. elektrické přepětí, extrémní teplota nebo rozlitá káva). U analogových systémů hraje fyzické zabezečení a jeho ochrana hlavní roli.

131. **Systémová a datová bezpečnost,** tj. ochrana před úmyslným nebo neúmyslným zásahem do běžného provozu, může zahrnovat:

- Ochrana celé infrastruktury systému videosledování (včetně vzdálených kamer, kabeláže a napájení elektřinou) proti fyzickému poškození nebo krádeži
- Ochrana přenosu záznamů komunikačními kanály zabezpečenými proti narušení
- Šifrování dat
- Používání hardwarových a softwarových řešení jako jsou firewally, antivirové systémy nebo systémy detekce kybernetických útoků
- Detekce selhání jednotlivých částí, softwaru a vzájemného propojení

[26] To může záviset na vnitrostátních zákonech a odvětvové regulaci.

- Prostředky obnovení dostupnosti a přístupu do systému v případě fyzického nebo technického incidentu.

Řízení přístupu zajišťuje, aby k systému a datům měly přístup pouze oprávněné osoby, zatímco ostatním je v tom zabráněno. Opatření, která podporují fyzickou a logickou kontrolu přístupu, zahrnují:

- Zajistit, aby všechny prostory pod videodohledem a veškeré uložené videozáznamy byly zabezpečeny proti neoprávněnému přístupu třetích stran
- Umístění monitorů takovým způsobem (zejména pokud jsou na otevřeném prostranství jako např. recepce), aby je mohli vidět pouze oprávnění operátoři
- Stanovení a vymáhání postupů pro udělení, změnu a odvolání fyzického a logického přístupu
- Implementace metod a prostředků ověřování a autorizace uživatelů, např. délka hesla a frekvence jeho změny
- Zaznamenávání a pravidelná kontrola činnosti prováděných uživateli jak v systému, tak s daty
- Průběžné monitorování a zjišťování neúspěšných přístupů a co možno nejrychlejší řešení zjištěných nedostatků

10 POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

132. Podle článku 35 (1) jsou správci povinni provádět posouzení vlivu na ochranu osobních údajů (DPIA), pokud je pravděpodobné, že daný typ zpracování dat může mít za následek vysoké riziko pro práva a svobody fyzických osob. Článek 35 (3) (c) stanoví, že správci musí vypracovat posouzení vlivu na ochranu osobních údajů, pokud zpracování představuje rozsáhlé systematické monitorování veřejně přístupných prostorů. Kromě toho je podle článku 35 (3) (b) je posouzení vlivu na ochranu osobních údajů požadováno také, pokud správce zamýšlí zpracovávat zvláštní kategorie údajů ve velkém měřítku.

133. Pokyny k posouzení vlivu na ochranu osobních údajů[27] poskytují další návody a podrobnější příklady relevantní pro videosledování (např. týkající se použití kamerového systému k monitorování chování řidičů na dálnicích). Článek 35 (4) vyžaduje, aby všechny dozorové úřady zveřejnily seznam druhů operací zpracování, které podléhají povinnému DPIA v jejich zemi. Tyto seznamy lze obvykle nalézt na webových stránkách příslušných úřadů. Vzhledem k typickým účelům videosledování (ochrana lidí a majetku, zjišťování, prevence a kontrola trestných činů, shromažďování důkazů a biometrická identifikace podezřelých) je důvodné předpokládat, že videodohled bude v mnoha případech vyžadovat DPIA. Správci dat by proto měli pečlivě prostudovat zmíněné dokumenty, aby byli schopni určit, zda je takové posouzení vyžadováno, a provést je, pokud je nezbytné. Výsledek provedeného DPIA by měl správci indikovat, jaká opatření na ochranu dat má provést.

[27] Pokyny k posouzení vlivu na ochranu osobních údajů (DPIA) stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679, wp248rev.01, http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=611236

134. Je také důležité uvést, že pokud výsledky DPIA ukáží, že zpracování by vedlo k vysokému riziku i přes správcem plánovaná bezpečnostní opatření, bude nezbytné konzultovat příslušný dozorový úřad ještě před zpracováním. Podrobnosti o předběžných konzultacích lze nalézt v článku 36.

Jménem Evropského sboru pro ochranu osobních údajů

Předsedkyně

(Andrea Jelinek)