Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky

Verze 2.0

Přijato dne 29. ledna 2020

Historie verzí

Verze 2.1	26. února 2020	Oprava věcné chyby
Verze 2.0	29. ledna 2020	Přijetí pokynů po veřejné konzultaci
Verze 1.0	10. července 2019	Přijetí pokynů k veřejné konzultaci

Obsah

Evropský sbor pro ochranu osobních údajů

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

s ohledem na Dohodu o EHP a zejména přílohu XI a protokol 37 k uvedené dohodě ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018[1],

s ohledem na články 12 a 22 svého jednacího řádu,

PŘIJAL TYTO POKYNY

1 ÚVOD

1. Intenzivní používání videotechniky má vliv na chování občanů. Rozsáhlé zavádění takových nástrojů ve značné míře v mnoha oblastech života vystaví jednotlivce dalšímu tlaku, pokud jde o zabránění odhalení toho, co by mohlo být vnímáno jako odchylka. Tyto technologie mohou *de facto* omezit možnosti anonymního pohybu a anonymního využívání služeb a obecně omezit možnost zůstat bez povšimnutí. To má dalekosáhlé důsledky v oblasti ochrany osobních údajů.

2. I když jednotlivcům nemusí vadit dohled pomocí videokamer zřízený například pro určité bezpečnostní účely, je třeba zaručit, aby se zabránilo zneužití pro zcela odlišné a – pro subjekt údajů – neočekávané účely (např. účely marketingu, sledování výkonnosti zaměstnanců atd.). Kromě toho je v současnosti zavedeno mnoho nástrojů pro využití pořízených snímků a přeměnu tradičních kamer na inteligentní kamery. Množství údajů generovaných videem v kombinaci s těmito nástroji a technologiemi zvyšuje rizika sekundárního využití (ať už se vztahují k účelu, který byl původně systému přiřazen, nebo nikoli), případně dokonce rizika zneužití. Pokud se jedná o dohled pomocí videokamer, je třeba vždy pečlivě zvážit obecné zásady uvedené v nařízení GDPR (článek 5).

3. Dohledové videosystémy v mnoha ohledech mění způsob, jakým odborníci ze soukromého i veřejného sektoru působí na soukromých nebo veřejných místech za účelem zvýšení bezpečnosti, získávání analýzy návštěvníků, poskytování personalizované reklamy atd. Dohledový videosystém se prostřednictvím stále častějšího zavádění inteligentní analýzy videa stal vysoce výkonným. Tyto technologie mohou narušovat soukromí více (např. složité biometrické technologie) nebo méně (např. jednoduché algoritmy počítání). Zůstat anonymní a zachovat si soukromí je obecně stále obtížnější. Otázky ochrany údajů, které vyvstávají v jednotlivých situacích, se mohou lišit, stejně tak se bude lišit právní analýza při použití technologie.

4. Kromě otázek ochrany soukromí existují také rizika spojená s možnými poruchami těchto zařízení a zaujatostí, kterou mohou vyvolat. Výzkumní pracovníci uvádějí, že software používaný k identifikaci, rozpoznávání nebo analýze obličeje funguje odlišně v závislosti na věku, pohlaví a etnickém původu osoby, jejíž totožnost zjišťuje. Algoritmy fungují na základě různých demografických údajů, a proto by

[1] Pokud se v tomto stanovisku hovoří o „členských státech”, rozumějí se tím „členské státy EHP“.

zaujatost při rozpoznávání obličeje mohla posílit předsudky ve společnosti. Z tohoto důvodu musí správci údajů rovněž zajistit, aby zpracování biometrických údajů pocházejících z dohledu pomocí videokamer podléhalo pravidelnému hodnocení z hlediska jeho relevance a dostatečnosti poskytnutých záruk.

5. Dohled pomocí videokamer není standardně nezbytností, pokud existují jiné prostředky k dosažení základního účelu. Jinak riskujeme změnu kulturních norem, která povede k akceptování nedostatku soukromí jako obecného předpokladu.

6. Účelem těchto pokynů je poskytnout návod, jak uplatňovat nařízení GDPR ve vztahu ke zpracování osobních údajů prostřednictvím videotechniky. Příklady nejsou vyčerpávající, obecné úvahy lze uplatnit na všechny potenciální oblasti použití.

2 OBLAST PŮSOBNOSTI[2]

2.1 Osobní údaje

7. Systematické automatizované monitorování konkrétního prostoru optickými nebo audiovizuálními prostředky, většinou pro účely ochrany majetku nebo ochrany života a zdraví jednotlivce, se v naší době stalo významným jevem. Tato činnost vede ke shromažďování a uchovávání obrazových nebo audiovizuálních informací o všech osobách vstupujících do monitorovaného prostoru, které lze identifikovat na základě jejich vzhledu nebo jiných charakteristických znaků. Na základě těchto údajů lze zjistit totožnost těchto osob. Tato činnost umožňuje také další zpracování osobních údajů o přítomnosti a chování osob v daném prostoru. Potenciální riziko zneužití těchto údajů roste v závislosti na rozměrech monitorovaného prostoru, jakož i na počtu osob, které jej navštěvují. Tato skutečnost se odráží v nařízení GDPR, a to v ustanovení čl. 35 odst. 3 písm. c), které vyžaduje provedení posouzení vlivu na ochranu osobních údajů v případě rozsáhlého systematického monitorování veřejně přístupných prostorů, jakož i v ustanovení čl. 37 odst. 1 písm. b), které vyžaduje, aby zpracovatelé jmenovali pověřence pro ochranu osobních údajů, pokud operace zpracování kvůli své povaze vyžaduje pravidelné a systematické monitorování subjektů údajů.

8. Nařízení se však nevztahuje na zpracování údajů, které neodkazují na osobu, např. pokud jednotlivec nemůže být přímo nebo nepřímo identifikován.

> Příklad: Nařízení GDPR se nevztahuje na falešné kamery (tj. jakékoli kamery, které nefungují jako kamery, a proto nezpracovávají žádné osobní údaje). *V některých členských státech však tato problematika může podléhat jiným právním předpisům.*
>
> Příklad: Záznamy z velkých výšek spadají do oblasti působnosti nařízení GDPR pouze tehdy, pokud zpracované údaje mohou být za určitých okolností spojeny s konkrétní osobou.
>
> Příklad: Součástí výbavy automobilu je videokamera pro poskytování pomoci při parkování. Pokud je kamera zkonstruována nebo seřízena tak, že neshromažďuje žádné informace týkající se fyzických osob (jako jsou poznávací značky nebo informace, které by mohly identifikovat kolemjdoucí), nařízení GDPR se nepoužije.

9.

2.2 Uplatňování směrnice o prosazování práva (směrnice (EU) 2016/680)

10. Směrnice (EU) 2016/680 se vztahuje zejména na zpracování osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.

2.3 Výjimka osobní či domácí činnosti

11. Podle čl. 2 odst. 2 písm. c) zpracování osobních údajů fyzickou osobou v průběhu výlučně osobních či domácích činností, mezi které mohou patřit i činnosti on-line, nespadá do oblasti působnosti nařízení GDPR.[3]

[2] EDPB poznamenává, že pokud to umožňuje nařízení GDPR, mohou se ve vnitrostátních právních předpisech uplatňovat zvláštní požadavky.

[3] Viz také 18. bod odůvodnění.

12. Toto ustanovení – tzv. výjimka osobní či domácí činnosti – je třeba v souvislosti s dohledem pomocí videokamer vykládat úzce. Podle názoru Evropského soudního dvora tedy musí být takzvaná „výjimka osobní či domácí činnosti“ „*vykládána tak, že se týká pouze činností 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*.“[4] Dále pokud dohledový videosystém zahrnuje neustálé zaznamenávání a ukládání osobních údajů a 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*[5].“

13. Pokud jde o videotechniku provozovanou v prostorech soukromé osoby, může spadat pod výjimku osobní či domácí činnosti. To závisí na několika faktorech, které je třeba zohlednit s cílem dospět k závěru. Kromě výše uvedených skutečností stanovených v rozsudcích Soudního dvora Evropské unie se uživatel dohledu pomocí videokamer v domácnosti musí zaměřit na to, zda má se subjektem údajů nějaký osobní vztah a zda rozsah nebo četnost dohledu nasvědčuje určité profesionální činnosti z jeho strany a možnému nepříznivému vlivu dohledu na subjekty údajů. Pokud platí kterákoli z výše uvedených skutečností, nemusí z toho nutně vyplývat, že zpracování nespadá do oblasti působnosti výjimky osobní či domácí činnosti. Aby to bylo možné určit, je nezbytné celkové posouzení.

> Příklad: Turista nahrává videozáznam jak prostřednictvím svého mobilního telefonu, tak prostřednictvím videokamery s cílem zdokumentovat svou dovolenou. Ukazuje záznamy přátelům a rodině, ale nezpřístupňuje je neurčitému počtu osob. Tento případ by spadal do oblasti působnosti výjimky osobní či domácí činnosti.
>
> Příklad: Závodnice ve sjezdu na horském kole chce zaznamenat svůj sjezd pomocí akční kamery. Jezdí na odlehlém místě a nahrávky plánuje používat pouze pro svou osobní zábavu doma. Tento případ by spadal do oblasti působnosti výjimky osobní či domácí činnosti, a to i tehdy, budou-li osobní údaje do určité míry zpracovány.
>
> Příklad: Někdo monitoruje svou vlastní zahradu a v této souvislosti pořizuje záznam. Prostor je oplocený a do zahrady pravidelně vstupuje pouze správce a jeho rodina. Tento případ by spadal do oblasti působnosti výjimky osobní či domácí činnosti za předpokladu, že v rámci dohledu pomocí videokamer nejsou pořizovány záznamy zahrnující, třebaže částečně, veřejný prostor ani sousední pozemek.

14.

[4] Rozsudek Soudního dvora ze dne 6. listopadu 2003, *trestní řízení proti Bodil Lindqvist*, C-101/01, bod 47.

[5] Rozsudek Soudního dvora ze dne 11. prosince 2014, *František Ryneš proti Úřadu pro ochranu osobních údajů*, C-212/13, bod 33.

3 ZÁKONNOST ZPRACOVÁNÍ

15. Před použitím musí být upřesněny účely zpracování (čl. 5 odst. 1 písm. b)). Dohled pomocí videokamer může sloužit mnoha účelům, jako je podpora ochrany majetku a jiných aktiv, podpora ochrany života a fyzické integrity jednotlivců, shromažďování důkazů pro občanskoprávní nároky.[6] Tyto účely monitorování by měly být zdokumentovány písemně (čl. 5 odst. 2) a je třeba je specifikovat pro každou provozovanou kameru. Kamery, které používá pro stejný účel jeden správce, lze dokumentovat společně. Subjekty údajů musí být dále informovány o účelu (účelech) zpracování v souladu s článkem 13 (*viz oddíl 7, Povinnosti týkající se transparentnosti a poskytování informací*). Dohled pomocí videokamer založený pouze na účelu „bezpečnosti“ nebo „pro vaši bezpečnost“ není dostatečně konkrétní (čl. 5 odst. 1 písm. b)). Kromě toho je v rozporu se zásadou, že osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem (viz čl. 5 odst. 1 písm. a)).

16. V zásadě může právní základ pro zpracování údajů získaných pomocí videokamer poskytovat kterýkoliv právní důvod podle čl. 6 odst. 1. Například pokud vnitrostátní právo stanoví povinnost provádět dohled pomocí videokamer, použije se čl. 6 odst. 1 písm. c).[7] V praxi se však s největší pravděpodobností použijí tato ustanovení:

- čl. 6 odst. 1 písm. f) (oprávněný zájem),
- čl. 6 odst. 1 písm. e) (nezbytnost splnit úkol prováděný ve veřejném zájmu nebo při výkonu veřejné moci).

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

3.1 Oprávněný zájem, čl. 6 odst. 1 písm. f)

17. Právní posouzení čl. 6 odst. 1 písm. f) by mělo vycházet z následujících kritérií v souladu se 47. bodem odůvodnění.

3.1.1 Existence oprávněných zájmů

18. Dohled pomocí videokamer je zákonný, je-li nezbytný pro účely oprávněného zájmu správce nebo třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů (čl. 6 odst. 1 písm. f)). Oprávněné zájmy správce nebo třetí strany mohou být právní[8], hospodářské nebo nehmotné.[9] Správce by však měl vzít v úvahu, že pokud subjekt údajů vznese námitku proti dohledu v souladu s článkem 21, správce může přistoupit k dohledu pomocí videokamer tohoto subjektu údajů, pouze pokud se jedná o *závažný* oprávněný zájem, který převažuje nad zájmy, právy a svobodami subjektu údajů, nebo pro určení, výkon nebo ochranu právních nároků.

---

[6] Pravidla shromažďování důkazů pro účely uplatnění občanskoprávního nároku se v jednotlivých členských státech liší.

[7] Tyto pokyny nerozebírají vnitrostátní právní předpisy, které se mohou v jednotlivých členských státech lišit, ani k nim neuvádějí podrobnosti.

[8] Rozsudek Soudního dvora ze dne 4. května 2017, *věc Rīgas satiksme*, C-13/16.

[9] Viz WP217, pracovní skupina zřízená podle článku 29.

19. Vzhledem k reálné a nebezpečné situaci může účel ochrany majetku proti vloupání, krádeži nebo vandalismu představovat oprávněný zájem pro dohled pomocí videokamer.

20. Oprávněný zájem musí být skutečný a musí být aktuální (tj. nesmí být smyšlený nebo spekulativní)[10]. Před zahájením dohledu musí existovat argument reálného ohrožení – jako třeba škody nebo vážné incidenty v minulosti. S ohledem na zásadu odpovědnosti se správcům doporučuje zdokumentovat relevantní incidenty (datum, povahu, finanční ztrátu) a související trestní obvinění. Tyto doložené incidenty mohou být přesvědčivým důkazem existence oprávněného zájmu. Existence oprávněného zájmu, jakož i nezbytnost monitorování by se měla přehodnocovat v pravidelných intervalech (např. jednou ročně, v závislosti na okolnostech).

> Příklad: Majitel obchodu si chce otevřít nový obchod a chce nainstalovat dohledový videosystém s cílem zabránit vandalismu. Pomocí statistik může prokázat, že v blízkém sousedství je vysoká pravděpodobnost výskytu vandalismu. Užitečné jsou také zkušenosti sousedních obchodů. Není nutné, aby dotčenému správci nejprve vznikla škoda. Pokud škody způsobené v sousedství svědčí o nebezpečí nebo podobných situacích, mohou poukazovat na oprávněný zájem. Nestačí však předložit vnitrostátní nebo obecnou statistiku trestné činnosti, aniž by byla provedena analýza dané oblasti nebo nebezpečí pro tento konkrétní obchod.

21.

22. Oprávněný zájem mohou představovat situace bezprostředního nebezpečí, které mohou nastat v bankách nebo obchodech s cenným zbožím (jako jsou klenotnictví) nebo oblastech, o nichž je známo, že jsou často dějištěm majetkových trestných činů (např. čerpací stanice).

23. Nařízení GDPR v čl. 6 odst. 1 druhé větě rovněž jasně uvádí, že orgány veřejné moci nemohou opírat své zpracování o důvody oprávněného zájmu, pokud plní své úkoly.

3.1.2 Nezbytnost zpracování

24. Osobní údaje by měly být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“), viz čl. 5 odst. 1 písm. c). Před instalací systému dohledu pomocí videokamer by měl správce vždy kriticky posoudit, zda je toto opatření zaprvé vhodné k dosažení požadovaného cíle a zadruhé přiměřené a nezbytné pro jeho účely. Opatření dohledu pomocí videokamer by měla být přijata, pouze pokud účel zpracování nelze přiměřeně splnit jinými prostředky, které méně zasahují do základních práv a svobod subjektu údajů.

25. Vzhledem tomu, že správce chce zabránit majetkovým trestným činům, může namísto instalace dohledového videosystému také přijmout alternativní bezpečnostní opatření, jako je oplocení prostor, zavedení pravidelných hlídek bezpečnostních pracovníků, najmutí vrátných, zajištění lepšího osvětlení, instalace bezpečnostních zámků, oken a dveří odolných proti násilnému otevření nebo nanesení povlaku nebo fólií proti graffiti na zdi. Tato opatření mohou být proti vloupání, krádeži a vandalismu stejně účinná jako dohledový videosystém. Správce musí podle konkrétního případu posoudit, zda taková opatření mohou být přiměřeným řešením.

[10] Viz WP217, pracovní skupina zřízená podle článku 29, s. 24 a násl. Viz také rozsudek Soudního dvora Evropské unie ve věci C-708/18, s. 44.

26. Před zahájením provozování kamerového systému je správce povinen posoudit, kde a kdy jsou opatření dohledu pomocí videokamer naprosto nezbytná. Systém dohledu, který funguje v noci i mimo běžnou pracovní dobu, obvykle splní potřeby správce, pokud jde o předcházení jakémukoli ohrožení majetku.

27. Obecně platí, že nezbytnost uplatnění dohledu pomocí videokamer k ochraně prostor správce končí na hranici nemovitosti.[11] Existují však případy, kdy monitorování nemovitosti k účinné ochraně nestačí. V některých individuálních případech může být nutné rozšířit dohled pomocí videokamer do bezprostředního okolí prostor nemovitosti. V této souvislosti by měl správce zvážit fyzické a technické prostředky, například zablokování nebo rozostření oblastí, které nejsou relevantní.

> Příklad: Knihkupectví chce chránit své prostory před vandalismem. Obecně by kamery měly zabírat pouze samotné prostory, protože pro splnění uvedeného účelu není nutné sledovat sousední prostory nebo veřejné prostory v okolí knihkupectví.

28.

29. Rovněž vyvstávají otázky týkající se nezbytnosti zpracování, pokud jde o způsob uchování důkazů. V některých případech může být nezbytné použít řešení černé skříňky, kde jsou záznamy po určité době uložení automaticky vymazány a přístup k nim je možný pouze v případě incidentu. V jiných situacích nemusí být nezbytné nahrávat jakýkoli videomateriál, ale vhodnější je namísto toho použít monitorování v reálném čase. Rozhodnutí mezi řešeními černé skříňky a monitorováním v reálném čase by mělo rovněž vycházet ze sledovaného účelu. Pokud je například cílem dohledu pomocí videokamer uchování důkazů, metody fungující v reálném čase obvykle nejsou vhodné. Někdy může být monitorování v reálném čase také rušivější než ukládání a automatické vymazávání materiálů po stanoveném časovém období (např. pokud někdo neustále sleduje obrazovku, může to být rušivější než v případě, že monitor vůbec neexistuje a materiály jsou uloženy přímo v černé skříňce). V této souvislosti je třeba zohlednit zásadu minimalizace údajů (čl. 5 odst. 1 písm. c)). Rovněž je třeba mít na paměti, že správce by mohl místo dohledu pomocí videokamer nasadit bezpečnostní pracovníky, kteří jsou schopni okamžitě reagovat a zasáhnout.

3.1.3 Vyvažování zájmů

30. Předpokládáme-li, že pro ochranu oprávněných zájmů správce je dohledový videosystém nezbytný, lze dohledový videosystém uvést do provozu, pouze pokud nad oprávněnými zájmy správce nebo třetí strany (např. ochrana majetku nebo fyzické integrity) nepřevažují zájmy nebo základní práva a svobody subjektu údajů. Správce musí zvážit, 1) do jaké míry má monitorování vliv na zájmy, základní práva a svobody jednotlivců a 2) zda způsobuje porušení nebo negativní důsledky s ohledem na práva subjektu údajů. Vyvažování zájmů je povinné. Základní práva a svobody na jedné straně a oprávněné zájmy správce na druhé straně je třeba pečlivě posoudit a vyvážit.

[11] V některých členských státech může tato problematika rovněž podléhat vnitrostátním právním předpisům.

Příklad: Soukromá parkovací společnost zdokumentovala opakující se problémy s krádežemi v zaparkovaných automobilech. Parkovací plocha je otevřený prostor a přístup k němu snadno získá kdokoli. Je však jasně označen značkami a silničními zábranami, které prostor obklopují. Parkovací společnost má oprávněný zájem (předcházení krádežím v automobilech zákazníků) monitorovat oblast během doby (během dne), kdy dochází k problémům. Subjekty údajů jsou monitorovány v omezeném časovém období, nejsou v oblasti pro rekreační účely a je také v jejich vlastním zájmu, aby se předešlo krádežím. Nad zájmem subjektů údajů nebýt monitorován v tomto případě převažuje oprávněný zájem správce.

Příklad: Restaurace se rozhodne instalovat videokamery na toalety s cílem kontrolovat čistotu hygienických zařízení. V tomto případě práva subjektů údajů jasně převažují nad zájmem správce, proto zde kamery nemohou být instalovány.

31.

3.1.3.1 Rozhodování podle jednotlivých případů

32. Vzhledem k tomu, že vyvažování zájmů je podle nařízení povinné, musí být rozhodnutí učiněno podle jednotlivých případů (viz čl. 6 odst. 1 písm. f)). Odkazování na abstraktní situace nebo srovnávání podobných případů je nedostatečné. Správce musí vyhodnotit rizika zasahování do práv subjektu údajů. Zde je rozhodujícím kritériem intenzita zásahu do práv a svobod jednotlivce.

33. Intenzitu lze mimo jiné určit podle typu shromažďovaných informací (obsah informací), rozsahu (hustota informací, prostorový a zeměpisný rozsah), počtu dotčených subjektů údajů, vyjádřeného buď konkrétním počtem, nebo podílem příslušné populace, dotčené situace, skutečných zájmů skupiny subjektů údajů, alternativních prostředků, jakož i povahy a rozsahu posuzování údajů.

34. Důležitými faktory vyvažování mohou být velikost sledované oblasti a množství sledovaných subjektů údajů. Použití dohledu pomocí videokamer v odlehlé oblasti (např. ke sledování volně žijících živočichů nebo k ochraně kritické infrastruktury, jako je rádiová anténa v soukromém vlastnictví), musí být posuzováno odlišně od dohledu pomocí videokamer na pěší zóně nebo v nákupním středisku.

Příklad: Pokud je nainstalována palubní kamera (např. za účelem shromažďování důkazů v případě nehody), je důležité zajistit, aby tato kamera nezaznamenávala nepřetržitě provoz, jakož i osoby, které se nacházejí v blízkosti silnice. Pokud tento požadavek není splněn, zájem mít k dispozici videozáznamy jako důkaz ve spíše teoretickém případě dopravní nehody nemůže odůvodnit tento závažný zásah do práv subjektů údajů.[11]

35.

3.1.3.2 Přiměřená očekávání subjektů údajů

36. Podle 47. bodu odůvodnění je třeba pečlivě posoudit existenci oprávněného zájmu. V této souvislosti je třeba uvést přiměřená očekávání subjektu údajů v daném okamžiku a v kontextu shromažďování jeho osobních údajů. Pokud jde o systematické monitorování, vztah mezi subjektem údajů a správcem se může výrazně lišit a může ovlivnit to, jaká přiměřená očekávání může subjekt údajů mít. Interpretace pojmu přiměřené očekávání by neměla vycházet pouze z dotčených subjektivních očekávání. Rozhodujícím kritériem musí být spíše to, zda by objektivní třetí strana mohla přiměřeně očekávat a dospět k závěru, že bude v této konkrétní situaci předmětem monitorování.

37. Například zaměstnanec na pracovišti většinou neočekává, že bude monitorován zaměstnavatelem.[12] Kromě toho není možné očekávat monitorování v soukromé zahradě, v obytných prostorech nebo ve vyšetřovnách a ošetřovnách. Stejně tak není rozumné očekávat monitorování v hygienických zařízeních nebo saunách – monitorování těchto oblastí je intenzivním zásahem do práv subjektu údajů. Přiměřená očekávání subjektů údajů jsou taková, že v těchto oblastech nebude probíhat žádný dohled pomocí videokamer. Na druhé straně může zákazník banky očekávat, že je monitorován uvnitř banky nebo bankomatem.

38. Subjekty údajů mohou rovněž očekávat, že nebudou monitorovány ve veřejně přístupných oblastech, zejména pokud se tyto oblasti obvykle používají k zotavení, regeneraci a volnočasovým činnostem, jakož i v místech, kde se jednotlivci zdržují a/nebo komunikují, jako jsou posezení, restaurace, parky, kina a tělovýchovná zařízení. V takových případech zájmy nebo práva a svobody subjektu údajů často převažují nad oprávněnými zájmy správce.

> Příklad: Na toaletách subjekty údajů očekávají, že nebudou monitorovány. Dohled pomocí videokamer, například s cílem předcházet nehodám, není přiměřený.

39.

40. Značky informující subjekt údajů o dohledu pomocí videokamer nemají při určování toho, co může subjekt údajů objektivně očekávat, žádný význam. To znamená, že se např. majitel obchodu nemůže spoléhat na to, že zákazníci budou mít *objektivně* přiměřená očekávání, že budou monitorováni, jen proto, že značka u vstupu informuje jednotlivce o dohledu.

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

41. Osobní údaje mohou být zpracovávány prostřednictvím dohledu pomocí videokamer podle čl. 6 odst. 1 písm. e), pokud je to nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce.[13] Může nastat případ, kdy výkon veřejné moci takové zpracování neumožňuje, ale jiné právní základy, jako je „bezpečnost a ochrana zdraví“ za účelem ochrany návštěvníků a zaměstnanců, mohou poskytnout omezený prostor pro zpracování, přičemž je stále nutné zohledňovat povinnosti a práva subjektu údajů podle nařízení GDPR.

42. Členské státy mohou ponechat v platnosti nebo zavést zvláštní vnitrostátní právní předpisy týkající se dohledu pomocí videokamer s cílem přizpůsobit uplatňování pravidel nařízení GDPR, a to přesnějším určením konkrétních požadavků na zpracování, pokud je to v souladu se zásadami stanovenými nařízením GDPR (např. omezení uložení, přiměřenost).

[12] Viz také: pracovní skupina zřízená podle článku 29, stanovisko 2/2017 ke zpracování údajů na pracovišti, přijaté dne 8. června 2017.

[13] Základ pro uvedené zpracování stanoví právo Unie nebo právo členského státu »a« toto zpracování musí být nezbytné pro splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je pověřen správce (čl. 6 odst. 3).

3.3 Souhlas, čl. 6 odst. 1 písm. a)

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

44. Pokud jde o systematické monitorování, může souhlas subjektu údajů sloužit jako právní základ v souladu s článkem 7 (viz 43. bod odůvodnění) pouze ve výjimečných případech. Povaha dohledu je taková, že tato technologie monitoruje neznámý počet osob současně. Správce bude stěží schopen prokázat, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů (čl. 7 odst. 1). Pokud subjekt údajů svůj souhlas odvolá, bude pro správce obtížné prokázat, že osobní údaje již nejsou zpracovávány (čl. 7 odst. 3).

> Příklad: Sportovci mohou během jednotlivých cvičení požadovat monitorování s cílem analyzovat své techniky a výkon. Na druhé straně, pokud sportovní klub začne z vlastního podnětu monitorovat za stejným účelem celý tým, nebude souhlas často platný, protože jednotliví sportovci mohou cítit tlak na udělení souhlasu, aby jejich odmítnutí souhlasu nepříznivě neovlivnilo spoluhráče.

45.

46. Pokud si správce přeje opírat se o souhlas, je jeho povinností zajistit, aby každý subjekt údajů, který vstoupí do oblasti, jež je pod dohledem pomocí videokamer, udělil souhlas. Tento souhlas musí splňovat podmínky článku 7. Vstup do označené monitorované oblasti (např. pokud jsou lidé vyzváni, aby vstoupili do monitorované oblasti tím, že projdou konkrétní chodbou nebo branou), nepředstavuje prohlášení či jiné zjevné potvrzení potřebné k souhlasu, pokud nesplňuje kritéria uvedená v článcích 4 a 7, jak je popsáno v pokynech k souhlasu.[15]

47. Vzhledem k nerovnováze mezi zaměstnavateli a zaměstnanci by se zaměstnavatelé ve většině případů neměli při zpracování osobních údajů opírat o souhlas, protože je nepravděpodobné, že bude dán svobodně. V této souvislosti by měly být zohledněny pokyny k souhlasu.

48. Právní předpis členského státu nebo kolektivní smlouvy, včetně „podnikových dohod“, mohou stanovit konkrétní pravidla pro zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním (viz článek 88).

[14] Pracovní skupina zřízená podle článku 29, „Pokyny k souhlasu podle nařízení 2016/679“ (WP 259 rev. 01). – schváleno EDPB.

[15] Pracovní skupina zřízená podle článku 29, „Pokyny k souhlasu podle nařízení 2016/679“ (WP 259) – schváleno EDPB – které by se měly zohlednit.

4 ZPŘÍSTUPNĚNÍ VIDEOZÁZNAMŮ TŘETÍM STRANÁM

49. Obecně se na zpřístupnění videozáznamů třetím stranám vztahují obecná ustanovení nařízení GDPR.

4.1 Zpřístupnění videozáznamů třetím stranám obecně

50. Zpřístupnění je definováno v čl. 4 odst. 2 jako přenos (např. individuální komunikace), šíření (např. zveřejnění on-line) nebo jakékoliv jiné zpřístupnění. Třetí strany jsou definovány v čl. 4 odst. 10. Pokud se zpřístupnění poskytuje třetím zemím nebo mezinárodním organizacím, uplatňují se také zvláštní ustanovení článku 44 a násl.

51. Jakékoli zpřístupnění osobních údajů je samostatným druhem zpracování osobních údajů, pro které musí mít správce právní základ uvedený v článku 6.

> Příklad: Správce, který chce nahrát záznam na internet, se musí při tomto zpracování opírat o právní základ, například získáním souhlasu subjektu údajů podle čl. 6 odst. 1 písm. a).

52.

53. Přenos videozáznamů třetím stranám pro jiný účel, než pro který byly údaje shromážděny, je možné podle pravidel uvedených v čl. 6 odst. 4.

> Příklad: Za účelem řešení škod je u závory (na parkovišti) nainstalován dohled pomocí videokamer. Dojde k poškození a záznam je předán právníkovi, který má ve věci jednat. V tomto případě je účel záznamu stejný jako účel předání.
>
> Příklad: Za účelem řešení škod je u závory (na parkovišti) nainstalován dohled pomocí videokamer. Záznam je zveřejněn on-line pouze z důvodů zábavy. V tomto případě se účel změnil a není slučitelný s původním účelem. Navíc by bylo problematické určit právní základ pro toto zpracování (zveřejnění).

54.

55. Příjemce třetí strany bude muset provést vlastní právní analýzu, zejména stanovit právní základ podle článku 6 pro zpracování (např. získání materiálu).

4.2 Zpřístupnění videozáznamů donucovacím orgánům

56. Zpřístupnění videozáznamů donucovacím orgánům je také nezávislým procesem, který vyžaduje samostatné odůvodnění správce.

57. Podle čl. 6 odst. 1 písm. c) je zpracování zákonné, pokud je nezbytné pro splnění právní povinnosti, která se na správce vztahuje. Přestože jsou platné policejní předpisy záležitostí, která je pod výlučnou kontrolou členských států, s největší pravděpodobností existují obecná pravidla, která upravují předávání důkazů donucovacím orgánům v každém členském státě. Zpracování správce předávajícího údaje upravuje nařízení GDPR. Pokud vnitrostátní právní předpisy vyžadují, aby správce spolupracoval s donucovacími orgány (např. v rámci vyšetřování), je právním základem pro předávání údajů právní povinnost podle čl. 6 odst. 1 písm. c).

58. Omezení účelu v čl. 6 odst. 4 je pak často problematické, protože zpřístupnění je výslovně založeno na právu členského státu. Zohlednění zvláštních požadavků na změnu účelu ve smyslu písmen a) až e) proto není nutné.

Příklad: Majitel obchodu pořizuje záznam u vchodu svého obchodu. Záznam ukazuje, jak někdo ukradl peněženku jiné osoby. Policie požádá správce o předání materiálu, aby pomohl při vyšetřování. V takovém případě by majitel obchodu použil pro zpracování převodu právní základ podle čl. 6 odst. 1 písm. c) (právní povinnost) ve spojení s příslušnými vnitrostátními právními předpisy.

59.

Příklad: V obchodě je z bezpečnostních důvodů nainstalována kamera. Majitel obchodu se domnívá, že v záznamu se objevilo něco podezřelého a rozhodne se odeslat materiál policii (bez jakékoli informace o tom, že probíhá nějaké vyšetřování). V tomto případě musí majitel obchodu posoudit, zda jsou splněny podmínky (ve většině případů) čl. 6 odst. 1 písm. f). Tento příklad obvykle nastane, pokud má majitel obchodu důvodné podezření, že byl spáchán trestný čin.

60.

61. Zpracování osobních údajů samotnými donucovacími orgány se neřídí nařízením GDPR (viz čl. 2 odst. 2 písm. d)), ale místo toho se řídí směrnicí o prosazování práva ((EU) 2016/680).

5 ZPRACOVÁNÍ ZVLÁŠTNÍCH KATEGORIÍ ÚDAJŮ

62. Dohledové videosystémy obvykle shromažďují velké množství osobních údajů, které mohou odhalit údaje velmi osobní povahy, a dokonce i zvláštní kategorie údajů. Zjevně lze data bez značného významu původně shromážděná prostřednictvím videozařízení použít k odvození jiných informací k dosažení jiného účelu (např. k mapování návyků jednotlivce). Dohled pomocí videokamer však není vždy považován za zpracování zvláštních kategorií osobních údajů.

> Příklad: Videozáznam ukazující, že subjekt údajů nosí brýle nebo používá invalidní vozík, nejsou samy o sobě považovány za zvláštní kategorie osobních údajů.

63.

64. Pokud se však videozáznam zpracovává za účelem vyvození zvláštních kategorií údajů, použije se článek 9.

> Příklad: Ze snímků zobrazujících identifikovatelné subjekty údajů, které se účastní akce, stávky atd. lze například odvodit politické názory. To by spadalo do působnosti článku 9.
>
> Příklad: Pokud by nemocnice instalovala videokameru za účelem sledování zdravotního stavu pacienta, považovalo by se to za zpracování zvláštních kategorií osobních údajů (článek 9).

65.

66. Obecně by se při instalaci dohledových videosystémů mělo pečlivě přihlížet k zásadě minimalizace údajů. I v případech, kdy se nepoužije čl. 9 odst. 1, by se tedy měl správce údajů vždy snažit minimalizovat riziko zachycení záznamu odhalujícího další citlivé údaje (nad rámec článku 9), a to bez ohledu na cíl.

> Příklad: Dohled pomocí videokamer zachycující kostel sám o sobě nespadá do působnosti článku 9. Správce však musí provést zvláště pečlivé posouzení podle čl. 6 odst. 1 písm. f), přičemž při posuzování zájmů subjektu údajů musí zohlednit povahu údajů a riziko zachycení dalších citlivých údajů (nad rámec článku 9).

67.

68. Pokud se pro zpracování zvláštních kategorií údajů používá dohledový videosystém, musí správce údajů identifikovat jak výjimku pro zpracování zvláštních kategorií údajů podle článku 9 (tj. výjimku z obecného pravidla, že se nemají zpracovávat zvláštní kategorie údajů), tak právní základ podle článku 6.

69. Například by teoreticky a ve výjimečných případech bylo možné použít čl. 9 odst. 2 písm. c) („[…] *zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby* […]“), správce údajů by to však musel odůvodnit jako absolutní nezbytnost chránit životně důležité zájmy osoby a prokázat, že daný „[…] subjekt údajů *není fyzicky nebo právně způsobilý udělit souhlas*“. Navíc správce údajů nebude moci systém používat z žádných jiných důvodů.

70. V této souvislosti je třeba poznamenat, že není pravděpodobné, že by každá výjimka uvedená v článku 9 byla odůvodněna zpracováním zvláštních kategorií údajů prostřednictvím dohledu pomocí videokamer. Konkrétněji se správci údajů, kteří tyto údaje zpracovávají v rámci dohledu pomocí videokamer, nemohou opírat o ustanovení čl. 9 odst. 2 písm. e), které umožňuje zpracování týkající se osobních údajů zjevně zveřejněných subjektem údajů. Pouhá skutečnost vstupu do oblasti dosahu kamery, neznamená, že subjekt údajů má v úmyslu zveřejnit zvláštní kategorie údajů, které se jej týkají.

71. Zpracování zvláštních kategorií údajů navíc vyžaduje zvýšenou a nepřetržitou obezřetnost při plnění určitých povinností; mezi ně patří v případě potřeby například vysoká úroveň zabezpečení a posouzení vlivu na ochranu osobních údajů.

> Příklad: Zaměstnavatel nesmí používat záznamy dohledu pomocí videokamer ukazující demonstraci s cílem identifikovat stávkující osoby.

72.

5.1 Obecné úvahy ohledně zpracování biometrických údajů

73. Používání biometrických údajů, a zejména rozpoznávání obličeje, s sebou nese zvýšená rizika pro práva subjektů údajů. Je zásadní, aby se tyto technologie používaly s náležitým ohledem na zásady zákonnosti, nezbytnosti, přiměřenosti a minimalizace údajů stanovené v nařízení GDPR. Vzhledem k tomu, že použití těchto technologií lze považovat za zvláště účinné, měli by správci nejprve posoudit vliv na základní práva a svobody a zvážit méně rušivé prostředky k dosažení jejich legitimního účelu zpracování.

74. Aby byly údaje považovány za biometrické podle definice v nařízení GDPR, musí zpracování nezpracovaných údajů, jako jsou fyzické či fyziologické znaky nebo znaky chování fyzické osoby, vyžadovat měření těchto znaků. Vzhledem k tomu, že biometrické údaje jsou výsledkem těchto měření, nařízení GDPR v čl. 4 odst. 14 uvádí, že se jimi rozumí osobní údaje *„[…] vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci […]*“. Videozáznamy jednotlivce však nemohou být samy o sobě považovány za biometrické údaje podle článku 9, pokud nebyly konkrétně technicky zpracovány s cílem přispět k identifikaci jednotlivce. [16]

75. Aby zpracování biometrických údajů bylo považováno za zpracování zvláštních kategorií osobních údajů (článek 9), je vyžadováno, aby tyto byly zpracovávány „za účelem jedinečné identifikace fyzické osoby“.

76. Stručně řečeno, s ohledem na čl. 4 odst. 14 a článek 9 je třeba zvážit tato tři kritéria:

- **povaha údajů:** údaje týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby,
- **prostředky a způsob zpracování**: údaje „vyplývající z konkrétního technického zpracování“,
- **účel zpracování:** údaje se musí použít za účelem jedinečné identifikace fyzické osoby.

77. Používání dohledu pomocí videokamer včetně funkce rozpoznání na základě biometrických údajů instalované soukromými subjekty pro jejich vlastní účely (např. marketing, statistika nebo dokonce bezpečnost) bude ve většině případů vyžadovat výslovný souhlas všech subjektů údajů (čl. 9 odst. 2 písm. a)), lze však použít i jinou vhodnou výjimku uvedenou v článku 9.

[16] 51. bod odůvodnění nařízení GDPR tuto analýzu podporuje a 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. […]*“.

Příklad: Za účelem zlepšení služeb soukromá společnost nahrazuje kontrolní stanoviště pro identifikaci cestujících na letišti (odbavení zavazadel, nástup na palubu) dohledovými videosystémy, které používají technologii rozpoznávání obličeje k ověření totožnosti cestujících, kteří k takovému postupu udělili souhlas. Jelikož zpracování spadá do oblasti působnosti článku 9, cestující, kteří již dříve udělili svůj výslovný a informovaný souhlas, se budou muset zaregistrovat například na automatickém terminálu, aby mohli vytvořit a zaregistrovat šablonu obličeje související s jejich palubní vstupenkou a totožností. Kontrolní stanoviště s rozpoznáváním obličeje musí být jasně oddělena, např. systém musí být nainstalován v bráně tak, aby nebyly zachyceny biometrické šablony osoby, která k tomu neudělila souhlas. Bránu vybavenou biometrickým systémem budou používat pouze cestující, kteří předtím udělili souhlas a zaregistrovali se.

Příklad: Správce řídí přístup do své budovy pomocí metody rozpoznávání obličeje. Lidé mohou tento způsob přístupu použít pouze tehdy, pokud předem udělili výslovný informovaný souhlas (podle čl. 9 odst. 2 písm. a)). Avšak s cílem zajistit, že nebude zachycen nikdo, kdo předtím neudělil svůj souhlas, by měl metodu rozpoznávání obličeje spouštět samotný subjekt údajů, například stisknutím tlačítka. S cílem zajistit zákonnost zpracování musí správce vždy nabídnout alternativní způsob přístupu do budovy bez zpracování biometrických údajů, jako jsou průkazy nebo klíče.

78.

79. V tomto typu případů, kdy jsou generovány biometrické šablony, musí správci zajistit, aby po dosažení výsledku „shoda“ nebo „žádná shoda“ všechny dočasné systematicky vytvořené šablony (s výslovným a informovaným souhlasem subjektu údajů) za účelem jejich srovnání se šablonami, které vytvořily subjekty údajů v době registrace, byly okamžitě a bezpečně vymazány. Šablony vytvořené pro registraci by měly být uchovány pouze pro realizaci účelu zpracování a neměly by být ukládány ani archivovány.

80. Pokud je však účelem zpracování například odlišit jednu kategorii osob od jiné, ale nikoliv jednoznačná identifikace určité osoby, pak toto zpracování nespadá do působnosti článku 9.

Příklad: Majitel obchodu by rád přizpůsobil svou reklamu podle pohlaví a věku zákazníka, což jsou znaky, které zachycuje dohledový videosystém. Pokud tento systém negeneruje biometrické šablony za účelem jednoznačné identifikace osob, ale namísto toho pouze zjišťuje tyto fyzické znaky za účelem klasifikace osoby, toto zpracování nespadá do působnosti článku 9 (pokud nedochází ke zpracování jiných typů zvláštních kategorií údajů).

81.

82. Článek 9 se však použije, pokud správce ukládá biometrické údaje (nejčastěji prostřednictvím šablon, které jsou vytvářeny pomocí extrakce podstatných prvků z nezpracované formy biometrických údajů (např. měření obličeje na základě snímku)) za účelem jedinečné identifikace osoby. Pokud si správce přeje zjistit, zda subjekt údajů znovu vstoupil do oblasti nebo vstoupil do jiné oblasti (například za účelem zobrazování pokračující přizpůsobené reklamy), potom by účelem byla jednoznačná identifikace fyzické osoby, což znamená, že by operace od začátku spadala do působnosti článku 9. Tento případ by mohl nastat, pokud správce ukládá generované šablony s cílem poskytovat další přizpůsobenou reklamu na několika billboardech na různých místech uvnitř obchodu. Protože systém používá fyzické znaky k detekci konkrétních jednotlivců, kteří se vracejí do dosahu kamery (jako návštěvníci nákupního centra), a sledují je, jedná se o metodu identifikace pomocí biometrických údajů, protože je zaměřena na rozpoznávání pomocí konkrétního technického zpracování.

Příklad: Majitel obchodu nainstaloval v obchodě systém rozpoznávání obličeje s cílem přizpůsobit reklamu jednotlivcům. Před použitím tohoto biometrického systému a poskytnutím přizpůsobené reklamy musí správce údajů získat výslovný a informovaný souhlas všech subjektů údajů. Systém by byl nezákonný, pokud by zachycoval návštěvníky nebo kolemjdoucí, kteří neudělili souhlas s vytvořením jejich biometrické šablony, i když je jejich šablona v co nejkratší době vymazána. Tyto dočasné šablony představují biometrické údaje zpracovávané za účelem jedinečné identifikace osoby, která nemusí chtít dostávat cílenou reklamu.

83.

84. EDPB podotýká, že některé biometrické systémy jsou nainstalovány v nekontrolovaných prostředích[17], což znamená, že zahrnují zachycení obličeje každého jednotlivce procházejícího v dosahu kamery, včetně osob, které s biometrickým zařízením nesouhlasily, a nesouhlasily tedy s vytvořením biometrické šablony. Tyto šablony jsou porovnány se šablonami vytvořenými u subjektů údajů, které udělily svůj předchozí souhlas během registrace (tj. uživatelé biometrického zařízení), aby správce údajů rozpoznal, zda je daná osoba uživatelem biometrického zařízení. V tomto případě je systém často navržen tak, aby rozlišoval jednotlivce, které chce v rámci databáze rozpoznat od těch, kteří nejsou zaregistrováni. Protože účelem je jedinečná identifikace fyzických osob, je pro jakoukoli osobu, kterou kamera zachycuje, nutná výjimka podle čl. 9 odst. 2 nařízení GDPR.

Příklad: Hotel používá dohled pomocí videokamer k automatickému upozornění správce hotelu, že dorazila osoba VIP, v okamžiku, kdy je rozpoznán obličej hosta. Tyto osoby VIP udělily předchozí výslovný souhlas s používáním rozpoznávání obličeje před tím, než byl pořízen jejich záznam v databázi zřízené za tímto účelem. Tyto systémy zpracování biometrických údajů by byly nezákonné, ledaže by všichni ostatní hosté monitorovaní (za účelem identifikace osob VIP) souhlasili se zpracováním podle čl. 9 odst. 2 písm. a) nařízení GDPR.

Příklad: Správce instaluje dohledový videosystém s rozpoznáváním obličeje u vchodu do koncertní síně, kterou spravuje. Správce musí zřídit jasně oddělené vstupy; jeden s biometrickým systémem a druhý bez něj (kde lze místo toho například naskenovat lístek). Vchody vybavené biometrickými zařízeními musí být nainstalovány a zpřístupněny způsobem, který zabrání systému zachytit biometrické šablony diváků, kteří k tomu neudělili souhlas.

85.

86. Pokud se souhlas vyžaduje podle článku 9 nařízení GDPR, správce údajů nesmí také podmínit přístup ke svým službám přijetím biometrického zpracování. Jinými slovy, a zejména pokud se biometrické zpracování používá pro účely autentizace, musí správce údajů nabídnout alternativní řešení, které nezahrnuje biometrické zpracování – bez omezení nebo dodatečných nákladů pro subjekt údajů. Toto alternativní řešení je rovněž vyžadováno pro osoby, které nesplňují omezení biometrického zařízení (je nemožné provést registraci nebo čtení biometrických údajů či zdravotní postižení osoby činí používání zařízení obtížným atd.), a pro případ nedostupnosti biometrického zařízení (například porucha zařízení). Musí být zavedeno „záložní řešení“ s cílem zajistit kontinuitu nabízené služby, které je však omezeno na výjimečné použití. Ve výjimečných případech může nastat situace, kdy je zpracování biometrických údajů hlavní činností služby poskytované na základě smlouvy, např. muzeum, které pořádá výstavu představující používání zařízení pro rozpoznávání obličeje. V takovém případě subjekt

[17] To znamená, že biometrické zařízení je umístěno v prostoru otevřeném pro veřejnost a je schopné pracovat v případě jakéhokoli kolemjdoucího, na rozdíl od biometrických systémů v kontrolovaném prostředí, které lze použít pouze na základě zapojení osoby, která k tomu udělila souhlas.

údajů nebude mít možnost odmítnout zpracování biometrických údajů, pokud se chce výstavy zúčastnit. V takovém případě je souhlas požadovaný podle článku 9 stále platný, pokud jsou splněny požadavky článku 7.

5.2 Navrhovaná opatření k minimalizaci rizik při zpracování biometrických údajů

87. V souladu se zásadou minimalizace údajů musí správci údajů zajistit, aby údaje extrahované z digitálního obrazu pro vytvoření šablony nebyly nepřiměřené a aby obsahovaly pouze informace požadované pro stanovený účel, čímž se zabrání jakémukoli dalšímu možnému zpracování. Měla by být přijata opatření, která zaručí, že šablony nelze předávat mezi jednotlivými biometrickými systémy.

88. Identifikace a autentizace/ověření pravděpodobně budou vyžadovat uložení šablony pro použití při pozdějším srovnání. Správce údajů musí zvážit nejvhodnější místo pro uložení údajů. V prostředí podrobeném kontrole (vymezené chodby nebo kontrolní stanoviště) se šablony musí ukládat na jednotlivá zařízení, která jsou v držení uživatele a nad kterými má výlučnou kontrolu (v chytrém telefonu nebo na průkazu totožnosti), nebo – pokud je to nutné pro konkrétní účely a existují-li objektivní potřeby – se musí ukládat v centralizované databázi v zašifrované podobě, přičemž klíč/heslo je výhradně pod kontrolou dané osoby, aby se zabránilo neoprávněnému přístupu k šabloně nebo místu uložení. Pokud se správce údajů nemůže vyhnout přístupu k šablonám, musí podniknout příslušné kroky k zajištění zabezpečení uložených údajů. To může zahrnovat šifrování šablony pomocí kryptografického algoritmu.

89. V každém případě musí správce přijmout veškerá nezbytná opatření k zachování dostupnosti, integrity a důvěrnosti zpracovávaných údajů. Za tímto účelem musí správce přijmout zejména tato opatření: rozdělit údaje během přenosu a ukládání, ukládat biometrické šablony a nezpracované údaje nebo údaje o totožnosti do různých databází, šifrovat biometrické údaje, zejména biometrické šablony, a vymezit zásady šifrování a správy klíčů, zavést organizační a technická opatření pro odhalování podvodů, přiřadit k datům kód integrity (například podpis nebo hodnotu hash) a zakázat jakýkoli externí přístup k biometrickým údajům. Tato opatření se budou muset vyvíjet spolu s rozvojem technologií.

90. Kromě toho by správci údajů měli mazat nezpracované údaje (snímky obličeje, znaky řeči, způsob chůze atd.) a zajistit účinnost tohoto vymazání. Pokud již neexistuje právní základ pro zpracování, musí být nezpracované údaje vymazány. Pokud biometrické šablony pocházejí z takových údajů, lze se domnívat, že sestavení databází by mohlo představovat stejnou, či dokonce větší hrozbu (protože nemusí být vždy snadné přečíst biometrickou šablonu bez znalosti toho, jak byla naprogramována, zatímco z nezpracovaných údajů lze sestavit jakoukoli šablonu). V případě, že by správce údajů potřeboval takové údaje uchovat, je třeba prozkoumat metody přidaného šumu (jako je vodoznak), což by mělo za následek, že vytvoření šablony by bylo neúčinné. Správce musí také vymazat biometrické údaje a šablony v případě neoprávněného přístupu ke koncovému zařízení pro porovnávání a čtení nebo k serveru úložiště a na konci životnosti biometrického zařízení vymazat všechny údaje, které nejsou užitečné pro další zpracování.

6 PRÁVA SUBJEKTU ÚDAJŮ

91. Vzhledem k charakteru zpracování údajů při používání dohledu pomocí videokamer je nutné objasnit některá práva subjektu údajů podle nařízení GDPR. Tato kapitola však není vyčerpávající, na zpracování osobních údajů prostřednictvím dohledu pomocí videokamer se vztahují všechna práva podle nařízení GDPR.

6.1 Právo na přístup

92. Subjekt údajů má právo získat od správce potvrzení, zda jeho osobní údaje jsou či nejsou zpracovávány. V případě dohledu pomocí videokamer to znamená, že pokud nejsou žádné údaje ukládány nebo předávány jakýmkoli způsobem, pak jakmile uplyne okamžik monitorování v reálném čase, může správce poskytnout pouze informaci o tom, že se žádné osobní údaje již nezpracovávají (kromě obecných povinností poskytování informací podle článku 13, viz *oddíl 7 – Povinnosti týkající se transparentnosti a poskytování informací*). Pokud se však údaje v době požadavku stále zpracovávají (tj. pokud se údaje ukládají nebo nepřetržitě zpracovávají jiným způsobem), měl by subjekt údajů získat přístup a informace v souladu s článkem 15.

93. Existuje však několik omezení, která se mohou v některých případech vztahovat na právo na přístup.

- Čl. 15 odst. 4 nařízení GDPR, nepříznivé dotčení práv a svobod jiných osob

94. Vzhledem k tomu, že ve stejné sekvenci dohledu pomocí videokamer může být zaznamenán jakýkoli počet subjektů údajů, její zhlédnutí by způsobilo další zpracování osobních údajů jiných subjektů údajů. Pokud si subjekt údajů přeje získat kopii materiálu (čl. 15 odst. 3), mohla by být nepříznivě dotčena práva a svobody jiného subjektu údajů v daném materiálu. S cílem zabránit těmto důsledkům by správce proto měl vzít v úvahu, že kvůli rušivé povaze videozáznamu by v některých případech neměl poskytovat videozáznamy, na kterých lze identifikovat jiné subjekty údajů. Ochrana práv třetích osob by však neměla být využívána jako výmluva s cílem zabránit oprávněným nárokům na přístup jednotlivců, správce by v těchto případech měl zavést technická opatření ke splnění žádosti o přístup (například úprava záznamu, jako je maskování nebo šifrování). Správci však nejsou povinni tato technická opatření zavádět, pokud mohou jiným způsobem zajistit, že jsou schopni reagovat na žádost podle článku 15 ve lhůtě stanovené v čl. 12 odst. 3.

- Čl. 11 odst. 2 nařízení GDPR, správce není schopen identifikovat subjekt údajů

95. Pokud ve videozáznamu nelze vyhledávat osobní údaje (tj. správce by pravděpodobně musel projít velké množství uloženého materiálu, aby nalezl dotčený subjekt údajů), nemusí být schopen identifikovat subjekt údajů.

96. Z těchto důvodů by subjekt údajů (kromě toho, že se identifikoval, a to včetně pomocí identifikačního dokladu nebo osobně) měl ve své žádosti adresované správci uvést, kdy – v přiměřené lhůtě, úměrně počtu zaznamenaných subjektů údajů – vstoupil do monitorované oblasti. Správce by měl předem informovat subjekt údajů o tom, jaké informace jsou potřebné k tomu, aby žádosti vyhověl. Je-li správce s to doložit, že není schopen identifikovat subjekt údajů, informuje o této skutečnosti subjekt údajů, pokud je to možné. V takové situaci by měl správce v rámci odpovědi subjekt údajů informovat o přesné oblasti monitorování, ověření kamer, které byly používány atd., aby subjekt údajů plně pochopil, které z jeho osobních údajů mohly být zpracovány.

Příklad: Pokud subjekt údajů požaduje kopii svých osobních údajů zpracovaných prostřednictvím dohledu pomocí videokamer při vstupu do nákupního centra, které navštíví 30 000 osob denně, měl by upřesnit, kdy prošel monitorovanou oblastí v časovém rámci přibližně jedné hodiny. Pokud správce materiál stále zpracovává, měla by být poskytnuta kopie videozáznamu. Pokud lze ve stejném materiálu identifikovat další subjekty údajů, měla by být před poskytnutím kopie subjektu údajů, který podal žádost, tato část materiálu anonymizována (například rozmazáním kopie nebo jejích částí).

Příklad: Pokud správce automaticky maže všechny záznamy, například do dvou dnů, správce není schopen po těchto dvou dnech subjektu údajů záznam poskytnout. Pokud správce po těchto dvou dnech obdrží žádost, měl by být subjekt údajů odpovídajícím způsobem informován.

97.

- Článek 12 nařízení GDPR, nepřiměřené žádosti

98. V případě nepřiměřených nebo zjevně neodůvodněných žádostí subjektu údajů může správce buď uložit přiměřený poplatek v souladu s čl. 12 odst. 5 písm. a) nařízení GDPR, nebo odmítnout žádosti vyhovět (čl. 12 odst. 5 písm. b) nařízení GDPR). Správce musí být schopen zjevnou neodůvodněnost nebo nepřiměřenost žádosti doložit.

6.2 Právo na výmaz a právo vznést námitku

6.2.1 Právo na výmaz (právo být zapomenut)

99. Pokud správce nadále zpracovává osobní údaje nad rámec monitorování v reálném čase (např. je ukládá), může subjekt údajů požádat o výmaz osobních údajů podle článku 17 nařízení GDPR.

100. Správce má povinnost na žádost bez zbytečného odkladu vymazat osobní údaje, pokud platí jedna z okolností uvedených v čl. 17 odst. 1 nařízení GDPR (a neuplatňuje se žádná z výjimek uvedených v čl. 17 odst. 3 nařízení GDPR). To zahrnuje povinnost vymazat osobní údaje, pokud již nejsou potřebné k účelu, pro který byly původně uloženy, nebo pokud je zpracování nezákonné (viz také *oddíl 8 – Doby uložení a povinnost provést výmaz*). Dále by v závislosti na právním základě zpracování měly být osobní údaje vymazány:

- *v případě souhlasu* kdykoli je souhlas odvolán (a neexistuje žádný jiný právní základ pro zpracování),
- v případě *oprávněného zájmu*:
  - kdykoli subjekt údajů uplatní právo vznést námitku (viz *oddíl 6.2.2*) a neexistují převažující závažné oprávněné důvody pro zpracování, nebo
  - v případě přímého marketingu (včetně profilování), kdykoli subjekt údajů vznese námitku proti zpracování.

101. Pokud správce videozáznam zveřejnil (např. prostřednictvím vysílání nebo streamování na internetu), je třeba podniknout přiměřené kroky s cílem informovat ostatní správce (kteří nyní zpracovávají příslušné osobní údaje) o žádosti podle čl. 17 odst. 2 nařízení GDPR. Přiměřené kroky by měly zahrnovat technická opatření s ohledem na dostupnou technologii a náklady na provedení. Pokud je to možné, měl by správce po výmazu osobních údajů v souladu s článkem 19 nařízení GDPR oznámit tuto skutečnost jednotlivým osobám, jimž byly osobní údaje dříve zpřístupněny.

102. Kromě povinnosti správce vymazat osobní údaje na žádost subjektu údajů je správce podle obecných zásad nařízení GDPR povinen omezit uložené osobní údaje (viz *oddíl 8*).

103. U dohledu pomocí videokamer je vhodné poznamenat, že například rozmazáním obrazu bez možnosti zpětné obnovit osobní údaje, které obraz dříve obsahoval, se osobní údaje v souladu s nařízením GDPR považují za vymazané.

> Příklad: Obchod se smíšeným zbožím má problémy s vandalismem, a to zejména na fasádě, a proto využívá dohled pomocí videokamer před vchodem přímo zaměřený na zdi. Kolemjdoucí požaduje, aby jeho osobní údaje byly od chvíle podání žádosti vymazány. Správce je povinen na žádost odpovědět bez zbytečného odkladu a nejpozději do jednoho měsíce. Vzhledem k tomu, že dotčený záznam již nesplňuje účel, pro který byl původně uložen (v době, kdy subjekt údajů prošel okolo obchodu, nedošlo k vandalismu), v době žádosti neexistuje žádný oprávněný zájem na uložení údajů, který by převažoval nad zájmy subjektů údajů. Správce musí osobní údaje vymazat.

104.

6.2.2 Právo vznést námitku

105. V případě dohledu pomocí videokamer založeného na *oprávněném zájmu* (čl. 6 odst. 1 písm. f) nařízení GDPR) nebo dohledu, který je nezbytný pro splnění úkolu prováděného ve *veřejném zájmu* (čl. 6 odst. 1 písm. e) nařízení GDPR), má subjekt údajů z důvodů týkajících se jeho konkrétní situace právo – kdykoli – vznést námitku proti zpracování v souladu s článkem 21 nařízení GDPR. Pokud správce neprokáže závažné oprávněné důvody, které převažují nad právy a zájmy subjektu údajů, musí se zpracování údajů jednotlivce, který vznesl námitku, ukončit. Správce by měl být povinen na žádost ze strany subjektu údajů odpovědět bez zbytečného odkladu a nejpozději do jednoho měsíce.

106. V souvislosti s dohledem pomocí videokamer by tato námitka mohla být vznesena buď při vstupu do monitorované oblasti, během pobytu v ní, nebo po jejím opuštění. V praxi to znamená, že pokud správce nemá závažné oprávněné důvody, monitorování oblasti, kde by bylo možné identifikovat fyzické osoby, je zákonné pouze tehdy, pokud:

    1) správce může na žádost okamžitě ukončit zpracování osobních údajů kamerou; nebo

    2) je monitorovaná oblast tak podrobně vymezena, aby správce mohl zajistit souhlas subjektu údajů před vstupem do oblasti, a nejedná se o oblast, ke které má subjekt údajů jako občan právo přístupu.

107. Cílem těchto pokynů není stanovit, co se považuje za *závazný* oprávněný zájem (článek 21 nařízení GDPR).

108. Při použití dohledu pomocí videokamer pro účely přímého marketingu má subjekt údajů právo na základě vlastního uvážení vznést námitku proti zpracování, protože právo vznést námitku je v této souvislosti absolutní (čl. 21 odst. 2 a 3 nařízení GDPR).

Příklad: Společnost má potíže s narušením bezpečnosti u svého vstupu pro veřejnost a používá dohled pomocí videokamer na základě oprávněného zájmu s cílem zachytit osoby, které do jejích prostor vstupují protiprávně. Návštěvník vznese námitku proti zpracování svých údajů prostřednictvím dohledového videosystému z důvodů týkajících se jeho konkrétní situace. Společnost však v tomto případě žádost odmítne s vysvětlením, že uložený záznam je potřebný z důvodu probíhajícího interního vyšetřování, a proto má závažné oprávněné zájmy pro další zpracování osobních údajů.

109.

7 POVINNOSTI TÝKAJÍCÍ SE TRANSPARENTNOSTI A POSKYTOVÁNÍ INFORMACÍ[18]

110. Nedílnou součástí evropských právních předpisů o ochraně údajů je již dlouhou dobu požadavek, že by si subjekty údajů měly být vědomy skutečnosti, že je v provozu dohled pomocí videokamer. O monitorovaných místech by subjekty údajů měly být podrobně informovány.[19] V rámci nařízení GDPR jsou obecné povinnosti týkající se transparentnosti a poskytování informací stanoveny v článku 12 a následujících článcích nařízení GDPR. Další podrobnosti jsou uvedeny v „Pokynech k transparentnosti podle nařízení 2016/679 (WP260)“ pracovní skupiny zřízené podle článku 29, které EDPB schválil dne 25. května 2018. V souladu s odstavcem 26 pokynů WP260 se použije článek 13 nařízení GDPR, pokud jsou osobní údaje získány „[…] od subjektu údajů sledováním (např. za použití zařízení na automatizovaný sběr dat nebo softwaru na zachycování dat, jako jsou kamery […]“).

111. Vzhledem k objemu informací povinně poskytovaných subjektu údajů mohou správci údajů zvolit vícevrstvý přístup, pokud se rozhodnou k zajištění transparentnosti použít kombinaci metod (odstavec 35 WP260, odstavec 22 WP89). Pokud jde o dohled pomocí videokamer, nejdůležitější informace by měly být uvedeny na samotném upozornění (první vrstva), zatímco další povinné údaje mohou být poskytnuty jinými prostředky (druhá vrstva).

7.1 Informace uvedené v první vrstvě (upozornění)

112. První vrstva se týká primárního způsobu, kterým správce poprvé seznamuje subjekt údajů s informacemi. V této fázi mohou správci použít upozornění, na kterém jsou uvedeny příslušné informace. Tyto informace mohou být doplněny ikonou s cílem poskytnout snadno viditelným, srozumitelným a jasným způsobem smysluplný přehled o zamýšleném zpracování (čl. 12 odst. 7 nařízení GDPR). Formát informací by měl být přizpůsoben umístění v jednotlivých případech (odstavec 22 WP89).

7.1.1 Umístění upozornění

113. Informace by měly být umístěny tak, aby subjekt údajů mohl snadno zjistit okolnosti dohledu před vstupem do monitorované oblasti (přibližně na úrovni očí). Není nutné odhalit umístění kamery, pokud není pochyb o tom, které oblasti podléhají monitorování, a jednoznačně se objasní souvislosti dohledu (odstavec 22 WP 89). Subjekt údajů musí být schopen odhadnout, kterou oblast kamera zachycuje, aby mohl předejít dohledu nebo v případě potřeby přizpůsobit své chování.

7.1.2 Obsah první vrstvy

114. Informace první vrstvy (upozornění) by obecně měly sdělovat nejdůležitější informace, např. podrobnosti o účelech zpracování, totožnost správce a existenci práv subjektu údajů, spolu s informacemi o nejvýznamnějších dopadech zpracování.[20] Mohou mezi ně patřit například oprávněné zájmy sledované správcem (nebo třetí stranou) a kontaktní údaje pověřence pro ochranu osobních údajů (připadají-li v úvahu). Musí také odkazovat na podrobnější druhou vrstvu informací a na to, kde a jak lze takové informace nalézt.

[18] Mohou se uplatňovat konkrétní požadavky podle vnitrostátních právních předpisů.

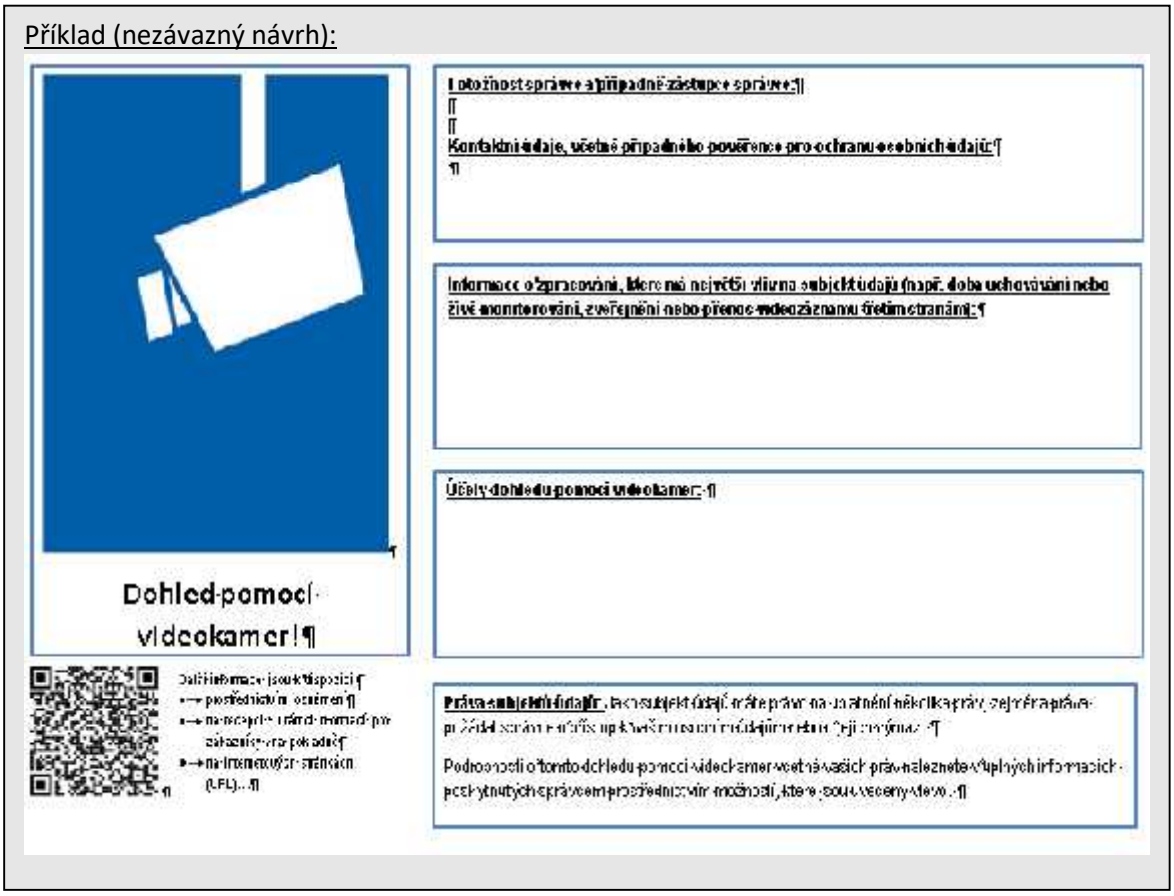
[19] Viz WP89, stanovisko 4/2004 pracovní skupiny zřízené podle článku 29 ke zpracování osobních údajů prostředky kamerového sledování.

[20] Viz odstavec 38 WP260.

115. Upozornění by mělo navíc obsahovat veškeré informace, které by mohly subjekt údajů překvapit (odstavec 38 WP260). Mohlo by se například jednat o přenosy třetím stranám, zejména pokud se nacházejí mimo EU, a dobu uložení. Pokud tyto informace nejsou uvedeny, subjekt údajů by měl mít možnost spoléhat se na to, že existuje pouze živé monitorování (bez zaznamenávání údajů nebo přenosu údajů třetím stranám).

116.

Příklad (nezávazný návrh):



7.2 Informace uvedené ve druhé vrstvě

117. Informace druhé vrstvy musí být rovněž zpřístupněny na místě snadno přístupném subjektu údajů, například jako úplný informační list dostupný v ústředním místě (např. informační přepážka, recepce nebo pokladna), nebo uvedeny na snadno přístupném plakátu. Jak je uvedeno výše, upozornění první vrstvy musí jasně odkazovat na informace druhé vrstvy. Kromě toho je optimální, pokud informace první vrstvy odkazují na digitální zdroj (např. kód QR nebo adresy internetových stránek) druhé vrstvy. Informace by však měly být snadno dostupné i nedigitálně. Mělo by být možné získat přístup k informacím druhé vrstvy bez vstupu do sledované oblasti, zejména pokud jsou informace poskytovány digitálně (toho lze dosáhnout například prostřednictvím odkazu). Dalším vhodným prostředkem by mohlo být číslo telefonní linky, na kterou lze zavolat. Informace však musí být poskytovány a musí obsahovat všechny povinné údaje podle článku 13 nařízení GDPR.

118. Kromě těchto možností a také s cílem zajistit větší účinnost, EDPB podporuje využívání technologických prostředků pro poskytování informací subjektům údajů. Mezi ně se může řadit například: určení zeměpisné polohy kamer a zaznamenání informací do mapových aplikací nebo internetových stránek, aby jednotlivci mohli na jedné straně snadno stanovit a specifikovat zdroje videa související s uplatněním jejich práv, a na druhé straně získat podrobnější informace o operaci zpracování.

Příklad: Majitel obchodu svůj obchod monitoruje. Pro dosažení souladu s článkem 13 stačí umístit upozornění na snadno viditelné místo u vchodu do obchodu, na kterém jsou uvedeny informace první vrstvy. Kromě toho musí poskytnout informační list obsahující informace druhé vrstvy u pokladny nebo na jakémkoli jiném ústředním a snadno přístupném místě v obchodě.

119.

8 DOBY ULOŽENÍ A POVINNOST PROVÉST VÝMAZ

121. Osobní údaje nesmí být uloženy po dobu delší, než je nezbytné pro účely, pro které jsou zpracovávány (čl. 5 odst. 1 písm. c) a e) nařízení GDPR). V některých členských státech mohou existovat zvláštní ustanovení týkající se dob uložení, pokud jde o dohled pomocí videokamer, v souladu s čl. 6 odst. 2 nařízení GDPR.

122. To, zda je nezbytné osobní údaje ukládat nebo ne, by se mělo kontrolovat v malém časovém rozmezí. Obecně je legitimním účelem dohledu pomocí videokamer často ochrana majetku nebo uchování důkazů. Obvykle lze vzniklé škody uznat do jednoho nebo dvou dnů. Pro usnadnění prokazování souladu s rámcem pro ochranu osobních údajů je v zájmu správce předem provést organizační opatření (např. v případě potřeby jmenovat zástupce pro prověřování a zabezpečení videomateriálu). S přihlédnutím k zásadám uvedeným v čl. 5 odst. 1 písm. c) a e) nařízení GDPR, konkrétně k minimalizaci údajů a omezení uložení, by se osobní údaje měly ve většině případů (např. za účelem odhalení vandalismu) vymazat, nejlépe automaticky, po několika dnech. Čím delší je doba uložení (zejména pokud je delší než 72 hodin), tím více důvodů musí být předloženo pro legitimitu účelu a nezbytnost uložení. Pokud správce používá dohled pomocí videokamer nejen pro monitorování svých prostor, ale má také v úmyslu údaje uložit, musí doložit, že k dosažení tohoto účelu je uložení údajů skutečně nezbytné. Pokud ano, musí být doba uložení jasně vymezena a individuálně stanovena pro každý konkrétní účel. Správce má povinnost stanovit dobu uchovávání v souladu se zásadami nezbytnosti a přiměřenosti a prokázat soulad s ustanoveními nařízení GDPR.

> Příklad: Majitel malého obchodu by si obvykle všiml vandalismu v tentýž den, kdy k němu došlo. V důsledku toho postačuje doba uložení v délce 24 hodin. Víkendy, kdy má obchod zavřeno, nebo delší období svátků však mohou být důvodem pro delší dobu uložení. Je-li zjištěna škoda, může majitel také potřebovat uložit videozáznam na delší dobu, aby mohl proti pachateli podniknout právní kroky.

123.

9 TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ

124. Jak je uvedeno v čl. 32 odst. 1 nařízení GDPR, zpracování osobních údajů při dohledu pomocí videokamer musí být nejen právně přípustné, ale správci a zpracovatelé jej také musí přiměřeně zabezpečit. Zavedená **organizační a technická opatření** musí být **přiměřená rizikům vůči právům a svobodám fyzických osob**, která vyplývají z náhodného nebo protiprávního zničení, ztráty, pozměňování či neoprávněného zpřístupnění údajů z dohledu pomocí videokamer nebo neoprávněného přístupu k nim. Podle článků 24 a 25 nařízení GDPR musí správci přijmout technická a organizační opatření také s cílem zajistit ochranu všech zásad týkajících se ochrany údajů při zpracování a stanovit prostředky, jejichž prostřednictvím mohou subjekty údajů uplatňovat svá práva, která jsou vymezena v článcích 15–22 nařízení GDPR. Správci údajů by měli přijmout interní rámec a zásady, které zajistí uplatňování těchto opatření jak v době stanovení prostředků pro zpracování, tak po dobu samotného zpracování, včetně případného vypracování posouzení vlivu na ochranu osobních údajů.

9.1 Co je dohledový videosystém

125. Dohledový videosystém[21] sestává z analogových a digitálních zařízení a softwaru za účelem zachycení snímků scény, zpracování snímků a jejich zobrazení pracovníkovi. Jeho součásti jsou uspořádány do těchto kategorií:

- prostředí související s videem: zachycování snímků, vzájemná propojení a zpracování snímků:
  - účelem zachycování snímků je vytvoření obrazu skutečného světa v takovém formátu, který lze použít ve zbývajících částech systému,
  - vzájemná propojení popisují veškerý přenos údajů v prostředí souvisejícím s videem, tj. připojení a komunikace. Příklady připojení jsou kabely, digitální sítě a bezdrátové přenosy. Komunikace popisují všechny videosignály a kontrolní datové signály, které mohou být digitální nebo analogové,
  - zpracování snímků zahrnuje analýzu, uložení a zobrazení snímku nebo posloupnosti snímků,
- z pohledu správy systému má dohledový videosystém tyto logické funkce:
  - správa údajů a správa činností, která zahrnuje zpracování příkazů pracovníka a činnosti generované systémem (postupy při alarmu, výstraha pro pracovníky),
  - mezi rozhraní k jiným systémům může patřit připojení k jiným bezpečnostním systémům (kontrola přístupu, požární poplach) a systémům pro jiné účely než zajištění bezpečnosti (systémy správy budov, automatické rozpoznávání registračních značek),
- zabezpečení dohledového videosystému spočívá v důvěrnosti, integritě a dostupnosti systému a údajů:
  - zabezpečení systému zahrnuje fyzické zabezpečení všech součástí systému a kontrolu přístupu k dohledovému videosystému,
  - zabezpečení údajů zahrnuje předcházení ztrátě údajů nebo manipulaci s údaji.

[21] Nařízení GDPR definici tohoto systému neuvádí, technický popis lze nalézt například v normě ČSN EN 62676-1-1:2014 Dohledové videosystémy pro použití v bezpečnostních aplikacích – část 1-1: Systémové požadavky.

126.

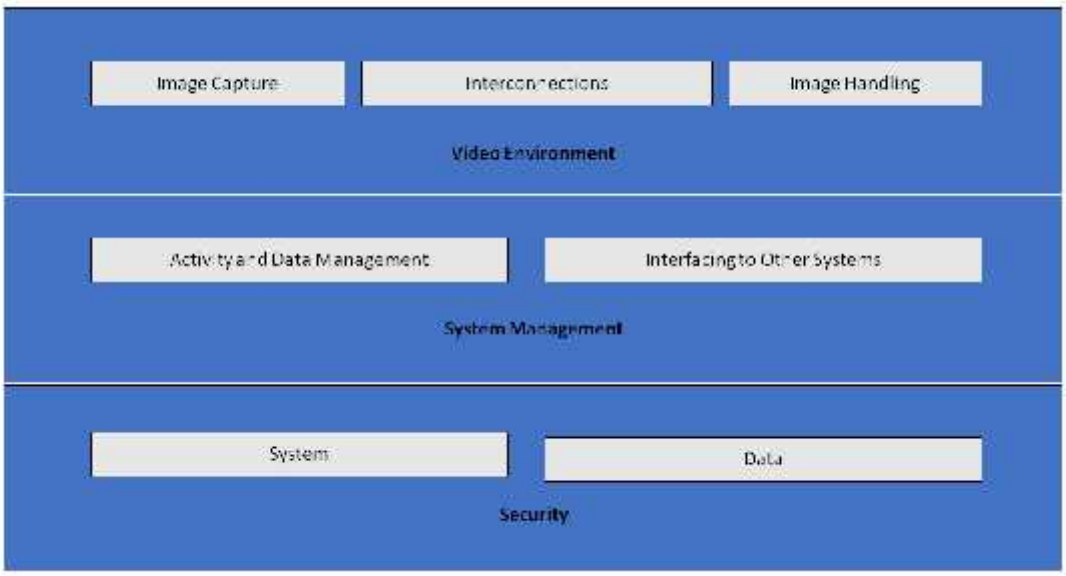


Image Capture	Zachycování snímků
Interconnections	Vzájemná propojení
Image Handling	Zpracování snímků
Video Environment	Prostředí související s videem
Activity and Data Management	Správa činností a údajů
Interfacing to Other Systems	Propojení s jinými systémy
System Management	Správa systému
System	Systém
Data	Údaje
Security	Bezpečnost

Obrázek 1– dohledový videosystém

9.2 Záměrná a standardní ochrana osobních údajů

127. Jak je uvedeno v článku 25 nařízení GDPR, správci musí zavést vhodná technická a organizační opatření k ochraně údajů již při plánování dohledu pomocí videokamer – před zahájením shromažďování a zpracování videozáznamu. Tyto zásady poukazují na potřebu zabudovaných technologií pro zvýšenou ochranu soukromí, výchozích nastavení, která minimalizují zpracování údajů, a poskytování nezbytných nástrojů umožňujících nejvyšší možnou ochranu osobních údajů[22].

128. Správci by měli zapracovat záruky ochrany údajů a soukromí nejen do konstrukčních specifikací technologie, ale také do organizačních postupů. Pokud jde o organizační postupy, měl by správce přijmout vhodný rámec řízení a stanovit a prosazovat zásady a postupy týkající se dohledu pomocí videokamer. Z technického hlediska by specifikace a konstrukce systému měly zahrnovat požadavky na zpracování osobních údajů v souladu se zásadami stanovenými v článku 5 nařízení GDPR (zákonnost zpracování, účel a omezení údajů, standardní minimalizace údajů ve smyslu čl. 25 odst. 2. nařízení GDPR, integrita a důvěrnost, odpovědnost atd.). Pokud správce plánuje získat komerční dohledový

[22] WP 168, stanovisko k dokumentu „Budoucnost soukromí“, společnému dokumentu pracovní skupiny zřízené podle článku 29 a pracovní skupiny pro policii a spravedlnost, jenž byl poskytnut jako příspěvek ke konzultaci Evropské komise ve věci právního rámce pro základní právo na ochranu osobních údajů (přijatého dne 1. prosince 2009).

videosystém, musí tyto požadavky zahrnout do nákupní specifikace. Správce musí zajistit dodržování těchto požadavků a musí je uplatňovat na všechny součásti systému a na všechny údaje zpracované tímto systémem po celou dobu jejich životního cyklu.

9.3 Konkrétní příklady vhodných opatření

129. Většina opatření, která lze použít k zajištění bezpečnosti dohledu pomocí videokamer, zejména pokud se používá digitální zařízení a software, se neliší od opatření používaných v jiných informačních systémech. Bez ohledu na zvolené řešení však musí správce přiměřeně chránit všechny součásti dohledového videosystému a údaje ve všech fázích, tj. během uložení (nepoužívané údaje), přenosu (přenášené údaje) a zpracování (používané údaje). Aby toho bylo možné dosáhnout, je nezbytné, aby správci a zpracovatelé zavedli jak organizační, tak technická opatření.

130. Při výběru technických řešení by měl správce zvážit technologie chránící soukromí také proto, že zvyšují bezpečnost. Jako příklad těchto technologií lze uvést systémy, které při poskytování videozáznamů subjektům údajů umožňují maskování nebo zakódování oblastí, které nejsou relevantní pro dohled, nebo odstranění snímků třetích osob.[23] Na druhé straně by vybraná řešení neměla poskytovat funkce, které nejsou nezbytné (např. neomezený pohyb kamer, funkce transfokátoru, rádiový přenos, analýza a schopnost pořizovat zvukové záznamy). Funkce, které jsou k dispozici, ale nejsou nezbytné, musí být deaktivovány.

131. K tomuto tématu je k dispozici velké množství literatury, včetně mezinárodních norem a technických specifikací, pokud jde o fyzické zabezpečení multimediálních systémů[24] a zabezpečení obecných informačních systémů[25]. Tento oddíl proto poskytuje pouze obecný přehled o tom tématu.

9.3.1 Organizační opatření

132. Kromě potřeby případného posouzení vlivu na ochranu osobních údajů (viz *oddíl 10*) by měli správci při vypracování vlastních zásad a postupů pro dohled pomocí videokamer zvážit tyto otázky:

- kdo je zodpovědný za správu a provoz dohledového videosystému,
- účel a rozsah projektu dohledu pomocí videokamer,
- vhodné a zakázané použití (kde a kdy je povolen dohled pomocí videokamer a kde a kdy povolen není; např. použití skrytých kamer a zaznamenávání zvuku kromě záznamu videa)[26],
- opatření v oblasti transparentnosti uvedená v *oddíle 7 (Povinnosti týkající se transparentnosti a poskytování informací),*
- způsob, jakým se video zaznamenává, a na jak dlouhou dobu se video zaznamenává, včetně ukládání videozáznamů souvisejících s bezpečnostními incidenty pro účely archivace,
- kdo musí absolvovat příslušnou odbornou přípravu a kdy,
- kdo má přístup k videozáznamům a za jakým účelem,
- provozní postupy (např. kdo a odkud monitoruje dohled pomocí videokamer, co dělat v případě incidentu porušení zabezpečení údajů),

---

[23] Použití těchto technologií může být v některých případech dokonce povinné pro dosažení souladu s čl. 5 odst. 1 písm. c). V každém případě mohou sloužit jako příklady osvědčených postupů.

[24] IEC TS 62045 – *Multimedia security - Guideline for privacy protection of equipment and systems in and out of use* (Zabezpečení multimédií – Pokyny pro ochranu soukromí u zařízení a systémů v provozu a mimo provoz).

[25] ISO/IEC 27000 – řada Systémy řízení bezpečnosti informací.

[26] Tyto otázky mohou záviset na vnitrostátních právních předpisech a odvětvových předpisech.

- jaké postupy musí dodržovat externí strany, aby mohly žádat o videozáznamy, a postupy pro zamítnutí nebo schválení takových žádostí,
- postupy pro pořizování, instalaci a údržbu dohledového videosystému,
- postupy pro řízení a obnovu v případě incidentů.

9.3.2 Technická opatření

133. **Zabezpečením systému** se rozumí **fyzické zabezpečení** všech součástí systému a integrita systému, tj. **ochrana před úmyslným a neúmyslným rušením jeho běžných operací a odolnost při tomto rušení** a **řízení přístupu**. Zabezpečením údajů se rozumí **důvěrnost** (k údajům mají přístup pouze osoby, kterým je přístup povolen), **integrita** (prevence ztráty údajů nebo manipulace s nimi) a **dostupnost** (v případě potřeby lze k údajům získat přístup).

134. **Fyzické zabezpečení** je nezbytnou součástí ochrany údajů a první linií obrany, jelikož chrání zařízení dohledového videosystému před krádeží, vandalismem, přírodní pohromou, katastrofami způsobenými člověkem a náhodným poškozením (např. způsobeným elektrickým přepětím, extrémními teplotami a rozlitou kávou). Při ochraně systémů založených na analogové technologii hraje fyzické zabezpečení hlavní úlohu.

135. **Zabezpečení systému a údajů**, tj. ochrana proti úmyslnému a neúmyslnému rušení jeho běžných operací, může zahrnovat:

- ochranu celé infrastruktury dohledového videosystému (včetně vzdálených kamer, kabeláže a napájení) před neoprávněnou fyzickou manipulací a krádeží,
- ochranu přenosu záznamu pomocí komunikačních kanálů zabezpečených proti odposlechu,
- šifrování údajů,
- použití hardwarových a softwarových řešení, jako jsou firewally, antivirové systémy nebo systémy detekce narušení, s cílem zabránit kybernetickým útokům,
- detekce poruch součástí, softwaru a vzájemných propojení,
- prostředky k obnovení dostupnosti systému a přístupu do něj v případě fyzických nebo technických incidentů.

136. **Řízení přístupu** zajišťuje, že k systému a údajům mají přístup pouze oprávněné osoby, zatímco ostatním je v přístupu k nim zabráněno. Mezi opatření, která podporují řízení fyzického a logického přístupu, patří:

- zajištění toho, aby všechny prostory, kde se provádí monitorování prostřednictvím dohledu pomocí videokamer a kde jsou uloženy videozáznamy, byly zabezpečeny proti nekontrolovanému přístupu třetích stran,
- umístění monitorů tak (zejména pokud se nacházejí v otevřených prostorách, jako je recepce), aby zobrazené údaje mohli vidět pouze oprávnění pracovníci,
- stanovení a uplatňování postupů pro udělování, změnu a zrušení fyzického a logického přístupu,
- metody a prostředky ověřování a schvalování uživatelů, včetně např. zavedení délky hesla a četnosti jeho změny,
- činnosti prováděné uživatelem (pokud jde o systém i údaje) se zaznamenávají a pravidelně kontrolují,
- monitorování a odhalování selhání přístupu se provádí nepřetržitě a identifikovaná slabá místa se řeší co nejdříve.

10 POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

137. Podle čl. 35 odst. 1 nařízení GDPR jsou správci povinni provést posouzení vlivu na ochranu osobních údajů, pokud je pravděpodobné, že určitý druh zpracování údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Čl. 35 odst. 3 písm. c) nařízení GDPR stanoví, že správci jsou povinni provést posouzení vlivu na ochranu osobních údajů, pokud zpracování představuje rozsáhlé systematické monitorování veřejně přístupných prostorů. Podle čl. 35 odst. 3 písm. b) nařízení GDPR se navíc posouzení vlivu na ochranu osobních údajů vyžaduje, pokud má správce v úmyslu provádět rozsáhlé zpracování zvláštních kategorií údajů.

138. Pokyny k posouzení vlivu na ochranu osobních údajů[27] poskytují další rady a podrobnější příklady týkající se dohledu pomocí videokamer (např. v souvislosti s „použitím kamerového systému pro monitorování chování řidičů na silnicích“). Čl. 35 odst. 4 nařízení GDPR vyžaduje, aby každý dozorový úřad zveřejnil seznam druhů operací zpracování, které podléhají povinnému posouzení vlivu na ochranu osobních údajů v jejich zemi. Tyto seznamy jsou obvykle k dispozici na internetových stránkách dozorových úřadů. Vzhledem k typickým účelům dohledu pomocí videokamer (ochrana osob a majetku, odhalování, prevence a omezování trestných činů, shromažďování důkazů a biometrická identifikace podezřelých) je rozumné předpokládat, že v mnoha případech bude dohled pomocí videokamer vyžadovat posouzení vlivu na ochranu osobních údajů. Správci údajů by proto měli tyto dokumenty pečlivě prostudovat s cílem zjistit, zda je takové posouzení požadováno, a v případě potřeby posouzení provést. Na základě výsledků provedeného posouzení vlivu na ochranu osobních údajů by správce měl zvolit příslušná opatření na ochranu osobních údajů ze strany správce.

139. Je rovněž důležité poznamenat, že pokud z výsledků posouzení vlivu na ochranu osobních údajů vyplývá, že zpracování by navzdory bezpečnostním opatřením plánovaným správcem mělo za následek vysoké riziko, bude nezbytné se před zpracováním obrátit příslušný dozorový úřad. Podrobnosti o předchozích konzultacích jsou uvedeny v článku 36.

Za Evropský sbor pro ochranu osobních údajů

předsedkyně

(Andrea Jelinek)

[27] WP248 rev.01, Pokyny k posouzení vlivu na ochranu osobních údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679 – schváleno EDPB.