Kamerový systém NetRex a GDPR

Nadpis druhé úrovně 10 kroků ke splnění GDPR v oblasti video dohledu

Základní informace

- General Data Protection Regulation (***GDPR*** nebo ***Obecné nařízení***) je nové obecné nařízení o ochraně osobních údajů v EU, které začne platit od 25. května 2018.
- GDPR má aplikační přednost před českým zákonem č. 101/2000 Sb., o ochraně osobních údajů. Přenáší mnohem více zodpovědnosti na samotné firmy, které s osobními daty zacházejí – a zavádí vysoké pokuty až 4 % z celkového ročního obratu.
- Podoba, chování a další vizuální prvky zachycené na videozáznamu, na základě kterých, může být osoba identifikována, se považují za osobní údaje, a GDPR se proto dotýká také provozovatelů kamerových systémů.
- Firmy obvykle potřebují řešit GDPR a ochranu osobních dat komplexně (včetně IT a bezpečnostních řešení a revize či přípravy související dokumentace), v tomto dokumentu se však zaměřujeme pouze na otázku video dohledu.
- Ačkoli byl tento dokument zpracován s právníky a specialisty na GDPR, lze očekávat další změny, úpravy a komentáře ze strany Úřadu pro ochranu osobních údajů. Sledujte proto aktualizace na stránkách **www.uoou.cz**

Jak naplnit požadavky GDPR v oblasti video dohledu a jak vám pomáhá řešení NetRex

1. Určete osobu, která je za váš kamerový systém zodpovědná

GDPR specifikuje roli správce, který nese hlavní zodpovědnost za nakládání s osobními údaji, a roli zpracovatele. Další osoba, tzv. pověřenec pro ochranu osobních údajů, je nutná pouze v případě, že je zpracovávání dat vaší hlavní činností, operujete se zvláštní kategorií forenzních osobních dat, nebo pokud jste veřejný subjekt.

Správce je povinen určit osobu, která je za data z kamerového systému zodpovědná a je schopna poskytnout monitorovaným osobám detailní informace týkající se shromažďovaných osobních údajů. Jméno konkrétní osoby musí být aktuální a dostupné, pokud jej někdo bude žádat.

Klienti a řešení NetRex:

- Správcem kamerového systému je vaše společnost, určete tedy konkrétního zaměstnance, který bude za video dohled zodpovědný. Je pravděpodobné, že tatáž osoba bude ručit i za

jiné oblasti zpracování osobních dat. Tato osoba je však zodpovědná pouze vůči vám v rámci jejího pracovního poměru. Vůči třetím osobám vždy ručí vaše společnost. Pokud je kamerový systém NetRex jediným nástrojem zpracování osobních dat ve vaší firmě, není nutný tzv. pověřenec.

- Zpracovatelem dat je společnost NetRex s.r.o. Jakožto specialisté na zpracování videozáznamu máme pověřence, jímž je k tomuto datu XY, kontakt V případě jakýchkoli otázek se na něj můžete obrátit.

Ivana Tomášová
pověřenec pro ochranu osobních údajů

ivana.tomasova@netrex.cz
tel.: +420 226 258 023

NetRex s.r.o.
U Nikolajky 9
150 00 Praha 5 – Smíchov

2. Proveďte inventuru kamer a test proporcionality

Provozovatel může provozovat kamerový systém ze 2 důvodů: (i) oprávněný zájem nebo (ii) je to vyžadováno zákonem. O oprávněný zájem se jedná, jestliže je zpracování nezbytné ve vztahu k účelu (např. ochrana majetku) a jestliže zájem správce převažuje nad základními právy a svobodami subjektů. Proto je třeba provést tzv. test proporcionality. **Tento požadavek není v GDPR nový, přesto ale doporučujeme u instalovaných kamer revizi tohoto základního posouzení provést.**

Klienti a řešení NetRex:

- Znovu si definujte důvody, proč u každé z instalovaných kamer převládá váš oprávněný zájem nad právy a svobodami monitorovaných osob (nejčastějším oprávněným důvodem pro pořizování kamerového systému je ochrana majetku a života či zdraví osob v prostorách provozovatele).
- Pro test proporcionality neexistuje jednoznačná definice pokrývající všechny případy, pomůže vám však např. komentář ÚOOÚ zde: https://www.uoou.cz/k-principu-proporcionality-pri-zpracovani-osobnich-udaju-na-zaklade-zakona-o-svobodnem-pristupu-k-informacim/d-5511/p1=1099
- **V případě, že je potřeba změnit umístění či nastavení některých kamer nebo byste měli pochybnosti o jejich správné instalaci, informujte zástupce NetRex**
- Výsledek interního testu zpracujte písemně, buď samostatně nebo v rámci dokumentu DPIA (níže)

3. Začněte vést záznam o činnostech zpracování

Záznamy o činnostech zpracování jsou záznamy, kterou budou správci osobních údajů podle GDPR povinni vést a na žádost je zpřístupnit dozorovému orgánu. Jsou jakousi náhradou za oznamovací povinnost Úřadu pro ochranu osobních údajů (***ÚOOÚ***), která byla Obecným nařízením zrušena.

GDPR vymezuje, jaké konkrétní údaje musí být součástí takové dokumentace o zpracování osobních údajů. Jsou to:

- jméno a kontaktní údaje správce
- účely zpracování
- rozsah zpracovávaných osobních údajů (popis kategorií subjektů údajů a kategorií osobních dat)
- informace o příjemcích daných osobních údajů
- informace o předávání údajů do třetích zemí
- informace o lhůtách pro výmaz jednotlivých kategorií údajů
- popis přijatých technických a organizačních opatření k zajištění bezpečnosti údajů

Klienti a řešení NetRex:

- Záznam o činnostech zpracování vám pomůžeme sestavit. Mějte ho stále aktuální a k dispozici.
- Některé informace se kryjí s dokumentem DPIA, o němž se zmiňujeme níže.

Ačkoli z této povinnosti existují určité výjimky,[1] doporučujeme našim klientům oba tyto záznamy, resp. dokumenty zpracovat.

[1] Z povinnosti vést záznamy o činnostech zpracování jsou vyloučeny podniky nebo organizace zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, představuje riziko pro práva a svobody subjektu údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií osobních údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů. Zpracování představuje riziko vždy, pokud jím může být způsobena nikoliv zanedbatelná újma dotčeným osobám. Půjde tak například o zpracování, které zahrnuje profilování nebo zpracování probíhající ve velkém měřítku. Rizikové je také zpracování osobních údajů, jejichž zneužití může vést ke krádeži identity či jinak přímo vést ke způsobení škody dotčené osobě. Zpracování je příležitostné, pokud k němu nedochází soustavně, ale naopak jde o zpracování jednorázové nebo pokud jde o zpracování, které je uskutečňováno ad hoc, případně v malém rozsahu a nepravidelně. Využívání kamerového systému nelze charakterizovat jako příležitostné.

4. Proveďte posouzení vlivu kamerového záznamu na ochranu osobních údajů (DPIA)

Správce má povinnost provést DPIA mj. v případě, že jde o „rozsáhlé systematické monitorování veřejně přístupných prostorů“.[2] V dokumentu vypracovaném společně s ÚOOÚ správce písemně specifikuje, z jakých oprávněných důvodů a pro jaké účely kamerový záznam pořizuje.

DPIA musí obsahovat alespoň: (i) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce; (ii) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelu; (iii) posouzení rizik pro práva a svobody subjektů údajů a (iv) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s GDPR, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Klienti a řešení NetRex:

- Pokud provádíte systematické monitorování (video dohled) například několika prodejen, je DPIA dokument povinný. Pomůžeme vám jej zpracovat společně s dozorovým orgánem.
- V případě dohledových kamer systému NetRex bude zřejmě nejčastějším oprávněným důvodem pro pořizování kamerového systému ochrana života, zdraví a majetku a osob v prostorách provozovatele.

5. Srozumitelně a stručně zveřejněte informace o činnosti kamerového systému

Správce má dle GDPR poskytnout monitorovaným osobám stručným, snadno dostupným a srozumitelným způsobem veškeré informace týkající se zpracování jejich osobních údajů.

V případě, že kamerovým systémem jsou sledování zaměstnanci, i oni musí být informování, nicméně invaze do jejich soukromí musí být minimální.

Vždy je potřeba vážit oprávněné zájmy správce a právo na soukromí sledovaných osob, tj. zda nepostačí k danému účelu kamerový systém bez zvukového záznamu či jiný, méně invazivní způsob, kterým dosáhnout chtěného účelu (test proporcionality). V každém případě je na tuto skutečnost vhodné upozornit při plnění informační povinnosti vůči sledovaným subjektům.

[2] Za veřejně přístupný prostor je třeba považovat jakékoliv místo, kam má přístup široký okruh individuálně neurčených lidí, třeba i za určitých podmínek a v určitou dobu.

Jaké informace musíte zveřejnit?

Všem monitorovaným osobám (tzv. subjektům údajů) musíte podle GDPR poskytnout tyto informace:

- totožnost a kontaktní údaje správce a případně jeho zástupce
- kontaktní údaje pověřence pro ochranu osobních údajů (pokud byl jmenován)
- účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování
- kategorie dotčených osobních údajů
- příjemce nebo kategorie příjemců osobních údajů
- doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby (jako přiměřená doba uchování videozáznamu se uvádí 30 dní)
- existenci práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz anebo omezení zpracování a práva vznést námitku proti zpracování, jakož i práva na přenositelnost údajů (zde je potřeba si uvědomit, že z povahy věci ne všechny práva subjektů údajů dle GDPR bude možné aplikovat na kamerové systémy; právo na přenositelnost může být jedním z takových práv)
- existenci práva podat stížnost u dozorového úřadu

Kdy je musíte zveřejnit?

Tyto informace musíte poskytnout nejpozději v okamžiku získání osobních údajů, tedy v okamžiku, kdy kamerový systém zachytí subjekt údajů.

Co když monitorujete zaměstnance?

V případě, že je kamerovým systémem monitorováno pracoviště, měli by všichni zaměstnanci být s touto skutečností obeznámeni – např. vnitřní směrnicí. Souhlas zaměstnanců nevyžadujte, neboť se jedná o zpracování osobních dat na základě oprávněných zájmů zaměstnavatele, nicméně invaze do soukromí zaměstnanců by měla být co nejmenší (test proporcionality).[3] Výše zmíněná informační povinnost platí i v tomto případě.

[3] Zákoník práce stanoví, že zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze jeho činnosti narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu apod. Každý zaměstnavatel by měl důkladně zvážit, zda je kamerový systém v daném provozu skutečně nutný, resp. zda zajištění tohoto účelu nelze dosáhnout jinými prostředky (test proporcionality). V případě, že by zaměstnavatel rád vedle obrazového záznamu pořizoval i ten zvukový, který by de facto snímal rozhovory dotčených osob, opět je potřeba toto důkladně zvážit, jelikož jde o velký zásah do soukromí zaměstnanců, který již nemusí být oprávněný. Výše uvedené lze vztáhnout i na osoby – nezaměstnance.

Jakým způsobem informace zveřejnit?

Ustanovení GDPR tvrdí „snadno dostupným a srozumitelným způsobem“. Pokud je kamerový záznam pořizován na veřejně přístupném místě, je vhodné ke všem vchodům umístit nálepku se základními informacemi a odkazem na web, kde podrobně informujete o všech aspektech zpracování dat z kamerového systému. Odkaz lze znázornit tzv. QR kódem. Rovněž se doporučuje mít k dispozici dokument obsahující veškeré informace ve fyzické podobě.

Příklad informace pro veřejnost v monitorovaném prostoru:

„Tento prostor je z důvodu ochrany osob a majetku monitorován kamerovým systémem se záznamem. Bližší informace o rozsahu a účelu zpracování osobních dat jsou k dispozici na webu www.firma.cz nebo přímo u správce: Karel Frištenský e-mail: varel@domena.cz tel. 777 777 777“.

Pokud je nainstalován kamerový systém, který neukládá záznam, ale funguje de facto pouze jako pohybové čidlo detekující procházející s tím, že nesnímá ani obličej ani jiné osobní údaje takto procházející či vstupující osoby, za účelem vyhodnocení návštěvnosti, v obecné rovině se nejedná o zpracování osobních údajů, a tudíž takový kamerový systém nepodléhá regulaci GDPR. Nicméně doporučujeme, aby alespoň zaměstnanci v daném prostoru byli odpovídajícím způsobem vyškoleni tak, aby byli schopni kvalifikovaně odpovědět na případně dotazy procházejících a byli jim schopni vysvětlit, že o žádné zpracování osobních údajů se v tomto případě nejedná. Samozřejmě vždy je možné do prostoru také umístit oznámení o existenci takového čidla s krátkým vysvětlením, že se nejedná o zpracování osobních údajů.

Upozorňujeme, že skryté sledování, tj. použití mechanismů záznamu pro získání údajů bez vědomí sledovaných osob je v zásadě nezákonné.

Klienti a řešení NetRex:

- Vytvořte si na vašem webu dokument s informací o zpracování osobních dat kamerovým systémem. Tento dokument vám pomůžeme sestavit podle vašich konkrétních specifik.
- Vylepte v každém monitorovaném prostoru nálepku s nápisem o přítomnosti kamerového systému, kterou vám dodáme.
- Vytvořte si doplňující nálepku/cedulku s konkrétními informacemi dle výše uvedeného příkladu.

6. Zajistěte kontrolu přístupu k osobním údajům (obrazu a nahrávkám z kamer)

Správce by měl přijmout opatření, která zabrání, aby k osobním datům měl přístup kdokoli např. volně z internetu. Proto je nutné:

a. specifikovat kdo a z jakého důvodu má přístup ke kamerám a záznamům z nich (tyto postupy ošetřit například ve vnitřní směrnici, jelikož půjde zejména o zaměstnance a zpracovatele).
b. zabránit (v rámci dostupných technických možností a nákladů) přístupu cizích osob, tzn. používat pro přístup silná hesla, v žádném případě nevystavovat, nesdílet nahrávky například na YouTube, Facebooku a podobně.

Klienti a řešení NetRex:

- Platforma NetRexu umožňuje efektivní řízení přístupu k jednotlivým kamerám a záznamům z nich.
- Je přísně stanoveno, kdo ze zaměstnanců NetRex je oprávněn mít přístup k datům zákazníků. Přístup helpdesku k nahrávkám a živému pohledu navíc musí povolit správce systému.
- Neustále pracujeme na zabezpečení platformy a reagujeme na aktuální hrozby aktualizacemi systému.
- Kamery komunikují se servery platformy přes šifrovaný TLS tunel. Autentizace je řádně provedena na obou stranách (server vůči zařízení i zařízení vůči serveru) tak, aby se

útočník nemohl vydávat za zařízení nebo server. Dále se z kamery odesílají data přes https spojení s ověřeným klientským certifikátem. *Poznámka: Tyto informace platí pro kamery s FW >= 5.60*

- Data mezi NetRex cloud platformou a klientem jsou výhradně přenášena pomoci šifrovaného https spojeni s důvěryhodnou certifikační autoritou. Náš HTTPS server je správně nakonfigurován, má hodnoceni A+ podle https://www.ssllabs.com/ssltest/analyze.html?d=system.netrex.cz&hideResults=on Používáme technologii HSTS pro vynucení šifrování dat.

7. Zabezpečte uchovávaná data proti odcizení/zneužití

Uložená osobní data by měla být chráněna vhodnými prostředky proti odcizení/zneužití. Tzn. data by měla být šifrována, pokud to není možné, mělo by být úložné zařízení uzamčeno a fyzicky chráněno proti odcizení, resp. měla by být přijatá dostatečná bezpečností opatření.

Klienti a řešení NetRex:

- Nahrávky a další data uživatelů jsou uložena na serverech patřící firmě NetRex. Tyto jsou hostovány ve 2 data centrech: Datacentrum Nagano, K Červenému dvoru 3156/25, Praha a Datacentrum TTC, Tiskařská 10, Praha. Obě datacentra mají certifikaci TIER III. K serverům mají přístup pouze autorizováni zaměstnanci firmy NetRex. Data zákazníků nejsou uložena mimo území EU. Servery jsou umístěny v uzamykatelném racku v datovém sále s řízeným přístupem a kamerovým systémem. Datový sál je umístěn v Datovém Centru, které splňuje bezpečnostní kritéria (ostraha 24/7, kontrola autorizovaných osob při vstupu, kontrola činností na sále pomocí kamerového systému). Obě datacentra se zavázaly splnit podmínky normy GDPR. Navíc jsou vaše nahrávky uložené v proprietárním formátu.
- Data na lokálním záznamovém zařízení NetRex Boxu jsou šifrovány asymetrickou šifrou (standard OpenPGP). Privátní klíč pro dešifrování se do boxu pošle ze survilla platformy pouze při autorizovaném požadavku na přístup k nahrávkám. Privátní klíč se nikdy neukládá na trvalé uložiště na boxu.
- V případě ukládání dat na SD kartu umožňují kamery Axis, které výhradně používáme, šifrovat nahrávky ukládané na SD kartu.

8. Umožněte, aby sledované osoby v záznamu mohly uplatnit právo na přístup k osobním údajům, případně výmaz těchto údajů

Sledovaná osoba má právo na:

- Právo být informována (viz. výše)
- na přístup:
    - Správce by měl na žádost subjektu o kopii vlastních osobních údajů ze záznamu (kde je uvedena přibližná doba a konkrétní datum/den, ve kterém byl jeho obraz zaznamenán) odpovědět do 1 měsíce. V případě ukládání dat na SD kartu umožňují kamery Axis, které výhradně používáme, šifrovat nahrávky ukládané na SD kartu.
    - Pokud se na vyžádaném záznamu objevují obrazy jiných osob než žadatele, správce přistoupí k úpravě záznamu-zakrytí/rozmazání/ztmavení snímky těchto ostatních osob před tím, než dodá záběry žadateli. Teoreticky může správce požádat o souhlas ostatních dotčených osob, co je ale v praxi nereálné.
    - Pokud záznam již neexistuje ke dni, kdy správce obdrží žádost, žadatel logicky nemůže získat kopii záznamu.[4]
    - Správce si může za službu poskytnutí záznamu účtovat přiměřený poplatek.
- na opravu;
- na výmaz:
    - Žádosti subjektů budou podávány zejména v případě další nepotřebnosti shromážděných a zpracovávaných údajů pro účely, ke kterým byly shromážděny a zpracovány.
    - Pokud zpracování již není potřebné pro dané účely, měl by správce zajistit výmaz sám. Lhůta, po kterou jsou údaje zpracovány je součástí výše uvedené informační povinnosti.
    - Před uplynutím této lhůty subjekt údajů nemůže požádat o výmaz, jelikož není splněna podmínka další nepotřebnosti.
    - Po uplynutí této lhůty o výmaz požádat lze, za předpokladu, že tak správce již neučinil.
    - Za rozumnou dobu uchování záběrů z kamer se považuje 30 dní.
    - Správce zakryje či jinak rozmaže snímek žadatele.

[4] Žadatelé by si měli být vědomi, že tyto záznamy jsou obvykle odstraňovány během jednoho měsíce od nahrávání.

Klienti a řešení NetRex:

- V případě žádosti o výmaz videozáznamu je možné tento záznam v platformě NetRex snadno vyhledat podle časové značky a smazat
- Je potřeba zpracovat a připravit dokumenty pro postupy při uplatňování práv data subjektů (vyřizování žádostí). Pomůžeme vám je připravit.

9. Zajistěte logování a ohlášení případných úniků dat/porušení zabezpečení dat

Další novou povinností vztahující se k GDPR je ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu. Správce oznámí porušení zabezpečení osobních údajů bezodkladně, nejlépe však do 72 hodin od okamžiku, kdy se o něm dozvěděl, příslušnému dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody subjektů údajů. Taktéž platí, že pokud zpracovatel zjistí porušení zabezpečení či únik dat, musí je bez zbytečného odkladu ohlásit správci.

Správce musí informovat ohledně porušení zabezpečení i samotné subjekty údajů, ale z této povinnosti existují široce pojaté výjimky, tj. správce nemusí subjekt údajů informovat, pokud uniklá data jsou nesrozumitelná, pokud přijal opatření snižující vysoké riziko pro práva a svobody fyzických osob, a pokud by to vyžadovalo nepřiměřené úsilí. Dozorový úřad může správci dodatečně tuto informační povinnost nařídit.

Ohlášení případů porušení zabezpečení osobních údajů dozorovému orgánu musí obsahovat alespoň: (i) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů; (ii) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace; (iii) popis pravděpodobných důsledků porušení zabezpečení osobních údajů a (iv) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Klienti a řešení NetRex:

- NetRex platforma je vybavena systémem pro logování provozu a operací. Ten slouží k detekci podezřelého chování, případně detekci kompromitace systému Záznamy z logů uchováváme po období 60 dnů až 2 roky dle typu a povahy operace.

- Je třeba připravit dokumenty pro ohlašování případných úniků dat dozorovému orgánu, subjektu údajů.

10. Zajistěte, že i subkontraktoři dodržují GDPR – nebo nemají k datům přístup

Je nutné, aby požadavky GDPR splňovali i všichni vaši dodavatelé, kteří by mohli mít přístup k záznamům. Za splnění požadavků odpovídáte ve vztahu k vámi monitorovaným subjektům vy. Doporučujeme tyto vzájemné vztahy upravit ve vzájemné smluvní dokumentaci mezi Vámi a dodavateli (smlouva o zpracování osobních údajů apod.)

Klienti a řešení NetRex:

- Nové povinnosti a skutečnosti mezi vámi (správcem údajů) a námi, společnosti NetRex s.r.o. (zpracovatelem údajů) upraví revidovaná smlouva, jejíž znění právě připravujeme. Upravenou smlouvu vám včas zašleme k prostudování a k podpisu.
- S výjimkou doby instalace nemají naši techničtí partneři k nahrávkám ani k živému pohledu z kamer přístup.