ELEKTRONICKÝ ZPRAVODAJ PRO POVĚŘENCE

HLÍDACÍ PES PRO OSOBY ZODPOVĚDNÉ ZA GDPR

Ukázkové číslo

Nový zákon o **zpracování osobních údajů**

V souvislosti s GDPR musí Česká republika přijmout nový zákon o zpracování osobních údajů (ZZOÚ), který jednak zruší stávající zákon o ochraně osobních údajů a jednak **upraví některé otázky, jež GDPR přímo neřeší** nebo v nichž jednotlivým státům umožňuje přísnější či méně přísnou úpravu.

Co upravuje nový zákon

ZZOÚ upravuje některé záležitosti, kde odkaz na místní legislativu stanoví přímo GDPR. ZZOÚ tak například rozšiřuje slučitelnost účelů i na situace, kdy je zpracování nezbytné a přiměřené **pro splnění povinnosti, která byla správci uložena**, nebo úkolu ve veřejném zájmu.

Návrh zákona se nyní projednává v Poslanecké sněmovně jako sněmovní tisk č. 138. Účinnosti by měl nabýt dnem vyhlášení ve Sbírce zákonů.

Dále stanoví, že **dítě nabude způsobilosti k udělení souhlasu** se zpracováním osobních údajů v souvislosti s nabídkou služeb informační společnosti **dovršením 15 let věku**.

Povinnosti správce, zpracovatele a práva subjektu lze, je-li to nezbytné a rozsahem přiměřené, **omezit k zajištění**:

- obranných a bezpečnostních zájmů ČR;
- předcházení, vyhledávání a odhalování trestné činnosti;
- stíhání trestných činů;
- výkonu trestu;
- veřejného pořádku a vnitřní bezpečnosti;
- jiného obecného veřejného cíle EU nebo členského státu (včetně daňových, měnových či rozpočtových záležitostí);
- dohledové, kontrolní nebo regulační funkce spojené s výkonem veřejné moci.

ZZOÚ stanovuje, která práva a povinnosti, v jakém rozsahu a za jakých podmínek lze omezit.

Osobní údaje v médiích, vědě a kultuře

ZZOÚ dále podrobněji řeší **výjimky pro zpracování osobních údajů pro novinářské účely nebo účely akademického, uměleckého či literárního projevu**, pokud zpracování slouží přiměřeným způsobem v nezbytném

POVINNOST JMENOVAT POVĚŘENCE

Pro účely povinnosti jmenovat pověřence pro ochranu osobních údajů se v ZZOÚ blíže definují veřejné subjekty jako orgány zřízené zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu. Bude se tak jednat například o notáře nebo exekutory.

rozsahu pro dosažení oprávněného cíle a převažuje-li tento zájem nad oprávněnými zájmy subjektu údajů.

V daném kontextu se řeší i **výjimky z poučovací a informační povinnosti správce a ochrana zdroje a obsahu informací**, jakož i **výjimky z práva subjektů na omezení zpracování** osobních údajů. Dochází rovněž k **omezení práva na námitku**, kdy subjekt musí prokázat, že nad zájmem na zveřejnění převažuje oprávněný zájem na ochraně jeho práv a svobod.

ZZOÚ dále stanoví pravidla pro **ochranu osobních údajů při předcházení, vyhledávání a odhalování trestné činnosti**, zajišťování veřejného pořádku a vnitřní i vnější bezpečnosti ČR. Jedná se o otázky, které GDPR vesměs neupravuje a odkazuje na národní legislativu. Tato ustanovení provádějí částečně směrnici č. 2016/680, o ochraně osobních údajů v trestní, soudní a policejní spolupráci.

Souhlas se zpracováním osobních údajů zůstane i nadále použitelný, ledaže by způsob jeho udělení nebyl v souladu s GDPR.

Zvláštní pravidla, částečně obsažená v ZZOÚ a částečně ve zvláštních předpisech, se vztahují i na **ochranu bezpečnostních a obranných zájmů ČR**. Bude se tak jednat především o zpravodajské složky a Národní bezpečnostní úřad.

Úřad pro ochranu osobních údajů

Další část ZZOÚ řeší postavení Úřadu pro ochranu osobních údajů (ÚOOÚ) jako ústředního správního úřadu. Ten bude mít i nadále působnost podle všech obecných předpisů na ochranu osobních údajů, vyjma dozoru nad zpravodajskými službami a určitými justičními orgány. Organizačně se nově zavádějí 2 místopředsedové úřadu a institut inspektorů se dále nepřejímá. Při své činnosti bude ÚOOÚ postupovat podle správního řádu. Navrhovaná podoba zákona je po prvním čtení v Poslanecké sněmovně a může se ještě změnit. ▪▪▪

Vzor ohlášení **dozorovému úřadu**

Správce má povinnost ohlašovat Úřadu pro ochranu osobních údajů každý případ porušení zabezpečení osobních údajů, ledaže je schopen prokázat a doložit, že je nepravděpodobné, že by dané porušení zabezpečení osobních údajů mělo za následek riziko pro práva a svobody fyzických osob.

Ohlášení je nutné učinit **bez zbytečného odkladu** poté, co se správce o porušení zabezpečení osobních údajů dozví, a je-li to možné, **do 72 hodin.** Není-li toto ohlášení možné učinit do 72 hodin, měly by být spolu s ním uvedeny důvody zpoždění. ▪▪▪

SPRÁVCE JE POVINEN V OHLÁŠENÍ UVÉST ALESPOŇ:

- **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;**
- **jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;**
- **popis pravděpodobných důsledků porušení zabezpečení osobních údajů;**
- **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.**

Není-li možné poskytnout informace současně, mohou být poskytnuty Úřadu pro ochranu osobních údajů postupně bez dalšího zbytečného odkladu.

Klikněte a stáhněte si formulář!

VZOR OHLÁŠENÍ DOZOROVÉMU ÚŘADU

Úřad pro ochranu osobních údajů
Pplk. Sochora 27
170 00 Praha 7

Věc: Ohlášení případu porušení zabezpečení osobních údajů

V souladu s ustanovením článku 33 Nařízení Evropského parlamentu a Rady (EU) č. 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 (obecné nařízení o ochraně osobních údajů) tímto ohlašuji Úřadu pro ochranu osobních údajů, že došlo k následujícímu porušení zabezpečení osobních údajů:

.....

.....

.....

.....

Porušením zabezpečení osobních údajů je dotčeno celkem ..... subjektů údajů, přičemž se jedná o následující subjekty údajů (resp. jejich kategorie):

.....

.....

Pravděpodobné důsledky porušení zabezpečení osobních údajů jsou následující:

.....

.....

S cílem vyřešit dané porušení zabezpečení osobních údajů a zmírnit možné nepříznivé dopady pro subjekty údajů bylo přijato nebo navrženo k přijetí následující opatření:

.....

.....

Kontaktním místem, kde může Úřadu pro ochranu osobních údajů zjistit bližší informace ohledně výše popsaného porušení zabezpečení osobních údajů, je:

.....

.....

V ..... dne .....

.....

Šifrování, anonymizace, pseudonymizace

Šifrování dat je proces, kterým se nezabezpečená elektronická data převádějí pomocí kryptografických postupů na data šifrovaná, **čitelná ideálně pouze pro majitele dešifrovacího klíče**. Šifrování dat slouží k jejich ochraně proti nežádoucímu zjištění cizí osobou a uplatňuje se při ukládání dat i při jejich přenosu, včetně přenosu přes telekomunikační sítě nebo internet.

CO LZE ŠIFROVAT?

- **data uložená v databázi;**
- **harddisky nebo vybrané adresáře v počítačích;**
- **komunikaci ve vnitřní síti;**
- **komunikaci na internetu.**

Šifrovací mechanismus

Pro každý případ se používá **jiný šifrovací mechanismus**:

- **Data uložená v databázi** – šifrování speciálními databázovými mechanismy – například Transparent Data Encryption u MS SQL;
- **Harddisky nebo adresáře v počítačích** – speciální nástroje pro šifrování celých disků (např. součástí Windows je nástroj BitLocker) nebo nástroje pro šifrování vybraných částí disku (např. součástí Windows je Encrypted File System);
- **Komunikace ve vnitřní síti** – ve vnitřní síti se obvykle považuje za dostačující využívání protokolů bránících odposlechu (např. se nemají používat starší protokoly FTP, TFTP, Telnet apod.) doplněné aplikací pravidel (access control listů) na aktivních prvcích; to je dále možné posílit prostřednictvím protokolů, které již byly navrženy jako šifrované (HTTPS, SFTP atd.);
- **Komunikace na internetu** – na internetu je možnost odposlechu, nebo dokonce úpravy komunikace obrovská; je proto nutné pro přenos osobních dat používat šifrované protokoly (HTTPS, IPSEC apod.).

Šifrovat lze i přenosová média (CD, USB flash disky, notebooky), takže v případě odcizení nejsou útočníkovi k ničemu.

Kdy šifrování je/není účinné?

Šifrování je účinné pro zamezení přístupu nepovolaných osob v podstatě ve všech částech zpracování a přenosu dat. Je však třeba si uvědomit, že každá část zpracování se šifruje jinak – **žádný způsob šifrování nechrání všechno**. Není účinné proti zpracování dat nad rámec zákona nebo proti odcizení dat ze strany odpovědných osob. Nevýhodou šifrování je **zvýšená režie** (prodlužuje zpracování dat, ubírá výpočetní výkon) a je také nutné přijmout opatření, jak se k datům dostat v případě havárie šifrování.

Anonymizace

Pojem anonymizace se v českém prostředí používá již dlouho. Principem je nahrazení pouze některých záznamů v databázi – těch, kde jsou obsažena osobní data. **Anonymizace je nevratný proces bez možnosti zpětné identifikace osoby**, tzn. data se nedají v budoucnu dohledat.

Anonymizace se používá například pro testování nových aplikací – zejména pro objemové testy, kdy je

PŘÍKLAD ANONYMIZACE A PSEUDONYMIZACE:

Máme spravovat následující osobní data:

ID	Jméno	Příjmení	Mzda	Adresa
54	Karel	Mach	18 000	Praha 1, Štupartská 6
55	Milan	Zamrazil	25 000	Praha 5, Na Bělidle 6
56	Karel	Winter	50 000	Praha 8, Novákových 13
57	Milan	Páv	12 000	Kladno, Železničářů 12

Anonymizovaná data mohou vypadat takto:

ID	Jméno	Příjmení	Mzda	Adresa
54	Karel	XXX	18 000	ZZZ
55	Milan	XXX	25 000	ZZZ
56	Karel	XXX	50 000	ZZZ
57	Milan	XXX	12 000	ZZZ

Jde o zjednodušený příklad s úmyslnou chybou – leccos by se jistě dalo poznat z výše mzdy. Bude například jasné, kdo z XXX je vedoucí, a vhodné není ani zachování stejného ID s původní tabulkou.

Naproti tomu pseudonymizovaná data se od sebe musejí ve všech polích lišit:

ID	Jméno	Příjmení	Mzda	Adresa
54	Karel	BOGOJ	18 000	99MAA
55	Milan	MAOAM	25 000	14BRT
56	Karel	KUTUL	50 000	55UVU
57	Milan	UUTAV	12 000	18STR

Aby se pseudonymizovaná data dala v budoucnu rozklíčovat a znovu zpracovávat, musí existovat převodní tabulka. Je vcelku jasné, že v daném případě bude vypadat nějak takto:

Příjmení	Klíč	Adresa	Klíč
Mach	BOGOJ	Praha 1, Štupartská 6	99MAA
Zamrazil	MAOAM	Praha 5, Na Bělidle 6	14BRT
Winter	KUTUL	Praha 8, Novákových 13	55UVU
Páv	UUTAV	Kladno, Železničářů 12	18STR

důležité ověřit, zda nová funkčnost zvládne existující objem dat. **Pro ochranu osobních dat se příliš nehodí:** data jsou sice zabezpečena, ale je obtížné je následně zrekonstruovat do použitelné podoby.

Pseudonymizace

Pseudonymizace je pojem hromadně používaný v nařízení GDPR. Jde o obdobu anonymizace, ovšem pseudonymizace je **procesem vratným**. Osobní údaje ve vybraných záznamech databáze jsou v tomto případě opět nahrazeny, ale je možné je v budoucnosti zrekonstruovat.

K rekonstrukci (odhalení) osobních údajů **je nutné mít klíč** (obvykle nějakou převodní tabulku či znalost nějakého algoritmu). Tuto převodní tabulku je samozřejmě nezbytné uchovat v absolutní tajnosti a **dostupná musí být jen zcela minimálnímu počtu osob**, v tomto případě obvykle databázovým administrátorům, protože rekonstrukce databáze může být pro běžného uživatele příliš náročná.

Pseudonymizace je účinná k **omezení (nikoliv úplnému zamezení) přístupu nepovolaných osob** v podstatě ve všech částech zpracování a přenosu dat. Proti šifrování **obvykle šetří čas**, pseudonymizovaná data se dají zpravidla ihned zpracovávat (v našem příkladu je okamžitě možné určit počet zaměstnanců a jejich průměrnou mzdu, aniž musíme pseudonymizovaná data rekonstruovat). Pseudonymizace **je částečně účinná proti zpracování dat nad rámec zákona**: pokud se správně navrhne, některé úkony se nepodaří na pseudonymizovaných datech realizovat.

Není účinná proti odcizení dat odpovědnými osobami. **Nevýhodou je extrémní citlivost převodních mechanismů**, navíc tyto mechanismy bývají méně dokonalé než šifrovací algoritmy. Často se používá u testů nebo při přenosech dat mimo organizaci – v tom případě obvykle ještě v kombinaci s šifrováním: Protistrana **dostane šifrovací klíč, ale nikoliv převodní mechanismy**. ▪▪▪

Poradna

Co s fotkami dětí, které už máme na webu školy řadu let a jejichž písemné souhlasy těžko odpovídají nařízení GDPR?

Pokud budeme postupovat striktně podle nařízení, měli bychom s účinností nařízení ukončit zpracování, ke kterému nemáme žádný právní titul, případně ke kterému máme souhlas v nevyhovující podobě. Jednou z možností je získat souhlas nový, ale je zřejmé, že v případě starých fotografií je získání nového souhlasu spojeno s velkým administrativním úsilím.

Je však potřeba občas použít selský rozum, pokud víme, že jsou na webu už řadu let a nikomu nikdy nevadily, a navíc není možné se k novému souhlasu dostat, je možné tyto fotky na webu ponechat, ovšem nesmíme fotografie šířit dál, prodávat či jinak s nimi nakládat. Měli bychom také rozlišovat, o jaké fotografie se jedná. Pokud půjde o fotografie ze společenských nebo sportovních akcí školy, lze předpokládat, že osoby zachycené na fotografii nebyly primárním předmětem focení, ale šlo o zaznamenání dané akce. Problém by nastal v případě portrétových fotografií zachycujících podobu konkrétního, identifikovatelného dítěte.

Je možné v osobních složkách zaměstnanců uchovávat kopie občanských průkazů či kartiček zdravotní pojišťovny?

Podobný postup se nedoporučuje. Jde sice o běžnou personální praxi, ale rozumnější je data si opsat. Při nástupu zaměstnance si tak zaměstnavatel jeho průkaz vypůjčí, opíše si do systému informace, které potřebuje, zároveň si je může překontrolovat a následně průkaz zaměstnanci vrátí.

Může mít firma víc pověřenců, každého pro jinou oblast působnosti (zvlášť pro personální agendu, obchodní agendu atd.)?

Obecně platí, že co není zakázáno, je dovoleno. Zřejmě tomu tedy nic nebrání, jejich činnost by však měla být koordinovaná, aby každý neuváděl něco jiného, protože do jisté míry se jejich činnosti shodují. ▪▪▪

Jak GDPR změní **fotografování a natáčení školních akcí?**

Fotografování žáků je často diskutovaným tématem i bez GDPR, které navíc už i tak nesnadnou pozici škol ještě komplikuje.

Obecně vzato je, a to platí i po účinnosti GDPR, nutné mít **souhlas zákonných zástupců** na to, aby mohlo být dítě fotografováno a jeho takto zpracovaná podoba dále užita. Souhlasy jsou dnes již standardně užívány v drtivé většině škol. Problémem jsou nové požadavky nařízení na parametry souhlasu. Je nutné provést revizi stávajících souhlasů a lze bohužel říci, že většina těch aktuálně užívaných požadavky GDPR nesplňuje.

Když už budete zajišťovat nový souhlas, je podle nařízení nutné dodržet následující podmínky: aby byl souhlas **svobodný, konkrétní, informovaný a jednoznačný**.

Předně není možné souhlasem podmínit poskytnutí jakékoli služby, souhlas je tedy věc dobrovolná a není na jeho udělení žádný právní nárok. Souhlas dále musí být konkrétní, a proto je nutné **vyžádat si souhlas pro zpracování a užití fotografie žáka pro jednotlivé účely** – tištěná fotografie na nástěnkách školky, na webových stránkách školky, případně na facebookovém profilu, pokud jej má školka zřízený.

Souhlas musí obsahovat také poučení subjektu údajů, že může souhlas kdykoli odvolat a jaká další práva subjekt údajů má. Například možnost vznést námitku proti zpracování nebo podat stížnost dozorovému úřadu. Novým právem subjektů je také **právo na výmaz**, které může subjekt údajů kdykoli u správce uplatnit, pokud má pocit, že zpracování je neoprávněné, nebo pokud subjekt údajů odvolal udělený souhlas.

Souhlasy doporučujeme získávat v písemné podobě, protože jinak není možné udělení souhlasu prokázat. Souhlas musí být dále jednoznačný, a proto je nutné, aby byl dostatečně **oddělen od ostatního sdělení**.

Jednoznačně nejlepší je samostatný list papíru, pokud by takové řešení bylo neekonomické, je možné připojit souhlas k jinému sdělení pouze za předpokladu, že bude zcela jednoznačné, že se osoba, která souhlas podepisuje, s jeho zněním seznámila. Tomuto požadavku lze vyhovět například tak, že bude souhlas vizuálně oddělen od ostatního sdělení, například rámečkem a samostatným polem pro podpis.

Souhlas je možné nechat udělit zákonné zástupce na dobu studia, nicméně je vhodné získat **nový souhlas na začátku každého školního roku**.

Je dobré si také dát pozor **na užívání nejrůznějších úložišť**, kam školky často nahrávají soubory fotografií ze školních akcí, aby k nim měli rodiče přístup. I když bývají tyto fotogalerie zajištěny heslem, nejsou všechna populární úložiště dostatečně zabezpečena proti neoprávněnému přístupu nebo nesplňují požadavky na **zabezpečení dat** podle nařízení.

Je vhodné poučit personál, aby nedocházelo k neoprávněnému zpracování podoby žáků. Problém totiž může představovat soukromá aktivita pedagogů, kdy se například učitelka školky vyfotí se svými žáky a umístí fotografii na svůj soukromý profil na sociální síti. Je třeba v takovém pří-

CO KDYŽ SOUHLAS K FOTOGRAFOVÁNÍ NEDOSTANEME?

Samozřejmě se zdá být logické takové žáky nefotit. Na druhou stranu existuje i názor, že fotografování není totéž, co zpracování podoby následným užitím fotografie, a tedy že vyloučení žáka z fotografování pro absenci souhlasu může být diskriminační. Pokud na takový výklad narazíte, jako řešení se nabízí technické opatření k znemožnění identifikace – tedy rozmazání nebo „rozkostičkování" obličeje žáka, k jehož fotografování nemáte souhlas. Jakkoli absurdní se takový výklad může zdát, řada škol a školek se s ním již setkala a v některé škole dokonce přišli s novinkou, kdy žákům, jejichž zákonní zástupci neudělili souhlas s fotografováním, nahrazují obličeje na fotkách známým obrázkem „smajlíka".

padě mít na paměti, že v případě učitelky v pracovní době se na takovou fotografii pravděpodobně **neuplatní výjimka z GDPR pro zpracování čistě osobní povahy**, pokud byla fotografie pořízena zaměstnancem správce během pracovní doby a během plnění jeho jiných pracovních povinností.

V případě souhlasů je dobré myslet při stanovení účelů i na **užití fotografií pro marketingové účely** v případě soukromých školek nebo na užití ve sdělovacích prostředcích, pokud by se školka rozhodla pochlubit se nějakou svou aktivitou v místních novinách. I na takové užití je nutný souhlas.

Existují i určité situace, kdy souhlas není nutný. Na mysli zde máme **fotografie ze školních akcí, které pořizují sami rodiče**. Jednak školka prakticky nemá možnost takovému focení zabránit, a hlavně v tomto případě se bude jednat o užití čistě osobní povahy, na které se GDPR nevztahuje.

Zákonný zástupce může poskytnout souhlas na celou dobu studia, ale je vhodné požádat o nový souhlas každý rok.

V rámci oficiálních školních focení je také vhodné zamyslet se nad množstvím osobních údajů, jež získá fotograf, kterého si do školky pozvete. Musíte se zamyslet nad tím, jaký máte s takovým fotografem vztah. Smluvní vztah nebude ve většině případů založen písemnou smlouvou, a tedy nikde nebude upravena povinnost mlčenlivosti nebo stav, kdy **fotograf může být dokonce v pozici zpracovatele** osobních údajů vůči školce, která si takové fotografa najme. Pokud si školka najme fotografa, tak školka jako správce určuje rozsah a účel zpracovávaných údajů a odpovídá tedy za bezpečnost zpracování osobních údajů. Fotograf musí tedy školce **zaručit, že bude postupovat v souladu s požadavky GDPR**.

Většina pravidel pro zpracování podoby se nijak razantně nemění, ale je nutné provést **revizi stávajících souhlasů**, projít si fyzicky budovu školky a podívat se, zda na nástěnkách nejsou fotografie, u kterých již dávno pominula doba uložení a zda také webové stránky školky neobsahují fotografie, které by bylo lepší vzhledem k GDPR odstranit.

V rámci procesních změn se musí školky připravit na způsob, jak reagovat na požadavky na výmaz, které mohou doprovázet odvolání souhlasu a jak o takových výmazech správně vést záznamy o činnostech zpracování, jinými slovy, jak vymazané údaje a fotografie evidovat. Další detaily jistě odhalí až praxe a výsledky kontrol ze strany úřadu. Nezbývá než doufat, že výsledky těchto kontrol povedou ke zpřesnění nejasných bodů a nebudou zároveň znamenat pro školky finanční pokuty. ▪▪▪

Elektronický zpravodaj pro pověřence | Vydavatel: Nakladatelství FORUM s.r.o. | Adresa redakce: Střelničná 1861/8a, 182 00 Praha 8 | Šéfredaktor: Mgr. Anna Zavadilová | Zákaznický servis: Pavlína Hrnková, office@forum-media.cz, tel: +420 251 115 576, fax: +420 251 512 422 | Jazyková redakce: Mgr. Jana Vašinová | Fotografie: www.bigstockphoto.com | Zlom časopisu: Renata Brtnická | Roční předplatné: 1990 Kč bez DPH | Objednávka předplatného: office@forum-media.cz, fax: +420 251 512 422, informace o předplatném: +420 251 115 576 | Redakční uzávěrka: 30. 5. 2018 | Elektronický zpravodaj vychází jako čtrnáctideník, celobarevný, 8 stran A4.