Zásady ochrany osobních údajů v souladu s GDPR

1. Základní pojmy GDPR

- Osobní údaj (OÚ) – jakákoliv informace, která se týká konkrétní fyzické osoby (subjektu údajů), ať už jde o identifikační a kontaktní údaje (např. jméno, příjmení, datum narození, adresa pobytu, rodné číslo, IČO/DIČ, telefonní číslo, e-mail, rovněž tak např. číslo klienta anebo spisová značka věci, pokud byla udělena), údaje o poloze, popisné údaje vypovídající o fyziologii člověka (např. výška, váha, velikost boty), informace z fotografií a kamerových záznamů, sociodemografické údaje (věk, pohlaví, rodinný stav, vzdělání, zaměstnání, příjmy a výdaje, počet dětí) nebo údaje o jeho chování a preferencích.
- Zvláštní kategorie osobních údajů (dříve citlivé osobní údaje) – některé osobní údaje zvlášť rizikové z pohledu možných zásahů do garantovaných práv a svobod fyzických osob, například údaje o zdravotním stavu, údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, genetické či biometrické údaje.
- Subjekt údajů – každá fyzická osoba, jejíž OÚ jsou zpracovávány.
- Zpracování – jakékoli nakládání s osobními údaji, např. shromáždění, zaznamenání, zpřístupnění, uložení, uspořádání, vyhledání, pozměnění, použití, šíření atd. Vedení spisové evidence (elektronické i listinné) a to jak v rámci klientské agendy, tak i administrativních činností (např. personalistika).
- Správce – jakákoli fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;
- Zpracovatel – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává pro správce osobní údaje, pokud ho tím správce pověří, a pouze ve správcem stanoveném rozsahu a ke stanoveným účelům; není vyloučeno, že jedna osoba bude zároveň správcem (například ve vztahu ke svým zaměstnancům) i zpracovatelem (ve vztahu k jinému správci).
- Společní správci – správci, kteří společně stanoví účely a prostředky zpracování OÚ.
- Příjemce – jakýkoli subjekt, kterému jsou osobní údaje poskytnuty (není rozhodující, zda přímo správcem, nebo zpracovatelem na pokyn správce), v některých případech se za příjemce nepovažují orgány veřejné moci.
- Právo vznést námitku – je-li zpracování založeno na oprávněném zájmu správce, případně prováděno ve veřejném zájmu nebo při výkonu veřejné moci, má subjekt údajů právo kdykoli proti takovémuto zpracování vznést námitku, subjekt údajů má právo vznést námitku také proti zpracování za účelem přímého marketingu a správce má v tomto případě povinnost dotčené OÚ dále nezpracovávat.
- ÚOOÚ – Úřad pro ochranu osobních údajů, kontrolní a dozorový úřad dle GDPR v ČR, se sídlem Pplk. Sochora 27, 170 00, Praha 7, telefon: +420 234 665 111, web: www.uoou.cz.
- Záznamy o činnostech zpracování – každý správce osobních údajů je povinen vést záznamy o činnostech zpracování osobních údajů, za něž zodpovídá. GDPR předepisuje formální vedení záznamů o činnostech zpracování především pro velké organizace (nad 250 zaměstnanců).
Nicméně, vzhledem k tomu, že záznamy musí vést i každý správce a zpracovatel (bez ohledu na počet zaměstnanců), pokud
a) prováděné zpracování OÚ pravděpodobně představuje riziko pro práva a svobody subjektů údajů,
b) zpracování OÚ není příležitostné, nebo
c) zpracování zahrnuje zpracování zvláštních kategorií údajů
týká se povinnost vést tyto formalizované záznamy všech , tedy jakékoli fyzické nebo právnické osoby, orgánu veřejné moci, agentury nebo jiného subjektu, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů, tedy s osobními údaji nakládá.
-DPO – pověřenec pro ochranu osobních údajů (z angl. data protection officer); DPO je jakýmsi interním auditorem zpracování a ochrany osobních údajů; dohlíží nad tím, že osobní údaje jsou zpracovávány a chráněny v souladu s GDPR. Povinnost jmenovat DPO není plošná – viz. ad. 4.3. níže (lze ho však ustavit dobrovolně).
- Analýza rizik – posouzení zpracování osobních údajů s cílem zjistit, jak závažná rizika plynou ze zpracování pro práva a svobody fyzických osob, a na základě toho přijmout opatření, která tato rizika minimalizují. Každá firma bude muset zpracovat analýzu rizik ve vztahu ke zpracováním osobních údajů, která provádí.

- DPIA – posouzení vlivu na ochranu osobních údajů (z angl. data protection impact assessment); formalizovaná riziková analýza, jejímž úkolem je zjistit, zda i přes vysoká rizika zpracování osobních údajů, zjištěná v rámci zpracování záznamů o činnostech zpracování, lze tyto údaje legálně zpracovávat za použití opatření, která sníží vysoká rizika na přijatelnou úroveň.
- Hlášení bezpečnostních incidentů – GDPR obsahuje povinnost správce hlásit porušení zabezpečení, integrity a ztrátu osobních údajů ÚOOÚ bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o nich dozvěděl; z této povinnosti jsou vyloučeny pouze incidenty s nízkou rizikovostí pro subjekty osobních údajů. Navíc správci musí oznámit toto porušení neprodleně všem dotčeným subjektům údajů, pokud je pravděpodobné, že příslušné porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob - viz ad. 4.5. níže

2. MINIMÁLNÍ POŽADAVKY NA SHODU S GDPR

Vzhledem k obsahu činnosti a s tím související nutnosti evidovat osobní údaje je nezbytné, aby došlo k naplnění přinejmenším požadavků minimální shody s GDPR:

- Vypracování dokumentace osvědčující naplňování zásad zpracování, ochrany a zabezpečení osobních údajů (OÚ) zejména podle čl. 5, 6, 25 a 32 GDPR – touto dokumentací bude vedle revize stávajících interních předpisů zejména vypracování pravidel IT bezpečnosti a pravidel bezpečného nakládání s dokumenty, včetně režimových a organizačních opatření, jakož i vypracování závazné dokumentace (interní směrnice) o zpracování osobních údajů. Součástí směrnice mohou být rovněž záznamy o činnosti zpracování (alternativně mohou být tyto záznamy samostatným dokumentem) - **viz. Příloha – VZOR Směrnice**

- Zavedení a popis přinejmenším jednoho generického procesu reakcí na práva subjektů osobních údajů – **viz. Příloha - VZOR žádosti subjektu údajů a odpovědi na žádost**
- Zavedení procesu naplňování informační povinnosti vůči subjektům osobních údajů
- Zavedení procesů identifikace, dokumentace a hlášení bezpečnostních incidentů na poli osobních údajů – blíže viz odst. 4.5. níže
- Revize smluv s dodavateli, kteří jsou zpracovateli osobních údajů – blíže viz. odst. 4.2. níže
- Systém sběru, evidence a zpracování souhlasů se zpracováním OÚ – blíže viz. odst. 4.4 níže

3. ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PODLE GDPR

Celé GDPR vychází z několika obecných zásad zpracování a ochrany osobních údajů. Tyto zásady jsou následující:
Zásada zákonnosti, korektnosti a transparentnosti znamená, že osobní údaje musejí být ve vztahu k subjektu údajů zpracovávány vždy korektně, zákonným a transparentním způsobem.
Zásada zákonnosti vyžaduje, aby osobní údaje byly zpracovávány na základě právem stanovených legitimních důvodů (právních titulů, které vymezuje čl. 6 GDPR)2, jimiž jsou: nezbytnost dodržení zákonné povinnosti, která se na správce vztahuje, nezbytnost pro splnění úkolů správce prováděných ve veřejném zájmu nebo při výkonu veřejné moci, **nezbytnost pro plnění smlouvy, jejíž stranou je subjekt údajů,** nebo za účelem přijetí opatření na žádost subjektu údajů před uzavřením smlouvy, nezbytnost pro účely oprávněných zájmů nebo zpracování založené na souhlasu subjektu údajů.
Se zásadou transparentnosti souvisí plnění informačních povinností vůči dotčeným subjektům údajů vymezených v čl. 12 až 14 GDPR. Firmy se s těmito povinnostmi setkají již při uzavírání smlouvy s klientem, v níž by mělo být pamatováno na poskytnutí informací klientům o zpracovávání jejich osobních údajů. Velmi vhodným místem pro naplnění informační povinnosti jsou rovněž webové stránky .
Zásada účelového omezení znamená, že každé zpracování osobních údajů musí být v souladu se svým legálním účelem. Osobní údaje musejí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný. Dostatečně určitě stanovený účel je např. „plnění smlouvy“nebo „plnění právní povinnosti“. Účel zpracování je výslovně vyjádřený, byl-li sdělen subjektům údajů. Legitimita účelu znamená, že je účel zpracování v souladu s právním řádem jako celkem, nikoliv tedy pouze v souladu s GDPR.
Zásada minimalizace údajů znamená, že je možné zpracovávat osobní údaje pouze v minimálním rozsahu,

počtu operací a množství evidencí, které jsou nezbytně nutné a potřebné pro splnění příslušného účelu zpracování. Ačkoliv tato zásada neznamená, že by měla existovat výlučně a pouze jedna evidence, každý správce musí usilovat o to, aby osobní údaje nebyly shromažďovány v rozsahu, který překračuje potřeby účelu (např. pro plnění smlouvy o dodávce školení shromažďovat rodná čísla účastníků školení), zpracovávány nadbytečnými procesy a operacemi, popř. rozmnožovány do většího množství evidencí, než je nutné (např. každý zaměstnanec si pořizuje svoji kopii spisu, aniž by pro to byly důležité provozní důvody).
Zásada přesnosti má vyjádření v povinnosti zpracovávat pouze přesná, správná a aktuální data. Znamená to, že v pravidelných časových intervalech (např. jednou za dva roky) by měla být osobní data klientů v databázi aktualizována, např. formou dotazu klientům, aby potvrdili správnost svých kontaktních údajů, případně je opravili. Také je vhodné upravit v interní směrnici o zpracování osobních údajů mechanismy a opatření určená k řízení životního cyklu sbíraných osobních údajů a vedoucí k včasné opravě a/nebo likvidaci nepřesných osobních údajů, jakož i postupy uplatňované v rámci aktualizace osobních údajů (zejména z podnětu subjektu údajů). Pravidelnost ověřování přesnosti a aktualizace osobních údajů by měla odpovídat potenciálnímu riziku vzniku újmy. Vyšší riziko vzniku újmy lze očekávat v případě pravidelného zpracovávání osobních údajů, než v případě jejich pouhého uložení.
Zásada omezeného uložení znamená povinnost uchovávat osobní údaje jen po dobu nezbytně nutnou k naplnění účelu zpracování. Tato zásada bude v praxi aplikována a splněna především dodržováním předepsaných archivačních lhůt klientských spisů a další dokumentace (finanční, účetní, zaměstnanecké). V rámci přípravy na GDPR je proto velmi vhodné provést revizi všech stávajících archivačních a skartačních lhůt podle příslušných agend a revidovat v této souvislosti stávající dokumentaci (pokud firma implementovala např. spisové a archivační řády).
Archivační (skartační) lhůty musejí být uvedeny v záznamech o činnostech zpracování osobních údajů a je nezbytné zajistit jejich dodržování. Subjekt údajů by měl být informován o době, po kterou budou jeho osobní údaje zpracovávány.
Zásada integrity a důvěrnosti představuje zejména povinnost zajistit bezpečné zpracování osobních údajů. Při posuzování vhodné úrovně bezpečnosti zpracování osobních údajů se zohlední zejména rizika, která představuje zpracování osobních údajů, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.
Vhodná technická a organizační opatření poměrně stručně zmiňuje čl. 32 GDPR.3 Standardizované postupy, vypracované za účelem zajištění náležité úrovně zabezpečení osobních údajů, případně včetně: a) pseudonymizace a šifrování osobních údajů; b) zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování; c) obnovení dostupnosti osobních údajů a přístup k nim včas v případě fyzických či technických incidentů; d) pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování, musejí být upraveny v interní směrnici o zpracování osobních údajů a figurovat v záznamech o činnostech zpracování.

4. SELF-ASSESSMENT

Jedná se o proces sebehodnocení z pohledu shody činnosti s požadavky GDPR. Výsledkem tohoto sebehodnocení by měla být identifikace úkolů, které příslušná firma musí splnit, aby dosáhla shody s GDPR.
V příloze je evidence zpracování osobních údajů s komentáři k vyplnění (Směrnice). Vyplněním tabulky by firma měla získat základní evidenci o zpracování osobních údajů, které provádí.
V bodě ad. 4.1. je pak obsažen popis práv subjektů údajů, které firma musí být připravena vyřizovat. V příloze jsou pak obsaženy vzory žádosti subjektu údajů a odpovědi na žádosti. Firma si tedy může ověřit, nakolik tyto požadavky splňuje, resp. čím musí doplnit své stávající procesy k dosažení shody s GDPR v tomto ohledu.
V části ad. 4.3. si firma může ověřit, zda má, či nemá povinnost jmenovat DPO (pověřence pro ochranu osobních údajů).
Část ad. 4.4. může pomoci firmě zkontrolovat si své souhlasy se zpracováním osobních údajů pro případy, kde je souhlas se zpracováním osobních údajů nutný.
Konečně na základě informací v části ad. 4.5. může firma do svých interních procesů začlenit do svých hlášení a oznamování bezpečnostních incidentů.

4.1 Vyřizování žádostí a stížností subjektů údajů

GDPR obsahuje řadu práv subjektů údajů. Firma musí zajistit hladký výkon těchto práv subjekty údajů. To bude pravděpodobně jedna z priorit ÚOOÚ při kontrolách shody s GDPR. Pro účely výkonu práv subjektů údajů lze proto uvést dvě základní doporučení:

- Firma musí pro účely shody s GDPR zajistit hladký výkon práv subjektů údajů, např. prostřednictvím online formulářů na svých webech nebo v listinné podobě přístupné v sídle firmy, či na pobočce
- Vyřizování všech žádostí subjektů údajů s tím, že by mělo být postupováno tak, aby bylo uplatnění práv subjektu co nejjednodušší a nejefektivnější. Usnadnit subjektům údajů výkon jejich práv lze dále např. implementací standardizovaných procesů (postupů) zakotvených v interních předpisech a uplatňovaných v případě podání příslušné žádosti subjektem údajů, jakož i ustanovením veřejně přístupného jednotného kontaktního místa pro uplatnění nároků subjektů údajů. Důležitý je rovněž pravidelný audit výkonu činností regulovaných GDPR, evidovaná kontrola organizačních opatření a činností zpracovatelů osobních údajů. Je-li jmenován pověřenec pro ochranu osobních údajů, vykonává v rámci činnosti správce osobních údajů výše uvedený audit, dohled a další kontrolní činnosti.
- Elektronické žádosti. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob. Vždy je třeba ověřit identitu toho, kdo žádost v elektronické formě podal, aby se informace nedostaly neoprávněným osobám (způsob a míra ověření by měly odpovídat kontextu, rozsahu a citlivosti požadované informace). K ověření je možné použít např. telefon nebo SMS klientovi, výjimečně lze požadovat i osobní identifikaci.
- Lhůta. Informace musí být poskytnuta bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit o dva měsíce, o čemž musí být subjekt údajů ze strany správce informován, včetně důvodů prodloužení.
- Poplatek. Zásadně platí, že informace se poskytují bezplatně. Pouze v případě, pokud jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, může správce buď uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost dokládá správce. Zneužitím nelze a priori rozumět výkon práv subjektu údajů.

V příloze - VZOR žádosti subjektu údajů a odpovědi na žádost.

4.1.1 Právo na přístup

Přístupem k osobním údajům se rozumí právo subjektu údajů získat od správce informaci (potvrzení), zda jsou či nejsou jeho osobní údaje zpracovávány a pokud jsou zpracovávány, má subjekt údajů právo tyto osobní údaje získat a zároveň má právo získat následující informace:

- účely zpracování,
- kategorie dotčených osobních údajů,
- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
- plánovaná doba, po kterou budou osobní údaje uloženy,
- že má právo požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku,
- že má právo podat stížnost u dozorového úřadu,
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
- o skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování.

Pokud správce o fyzické osobě žádné údaje nezpracovává, poskytuje se informace, že osobní údaje tazatele nejsou předmětem zpracování osobních údajů ze strany správce.

I zamítnutí žádosti musí být vyřízeno ve stanovené lhůtě.

4.1.2 Právo na výmaz

Právo na výmaz představuje povinnost správce zlikvidovat osobní údaje, které o žadateli zpracovává, pokud je splněna alespoň jedna podmínka:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,
- subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,

- osobní údaje byly zpracovávány protiprávně,
- osobní údaje musí být vymazány ke splnění právní povinnosti,
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 GDPR.

Výše uvedené podmínky se neuplatní, pokud je zpracování OÚ nezbytné:
a) pro určení, výkon nebo obhajobu právních nároků;
b) pro výkon práva na svobodu projevu a informace;
c) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;
d) z důvodu veřejného zájmu v oblasti veřejného zdraví podle GDPR;
e) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely podle GDPR, pokud je pravděpodobné, že by právo na výmaz znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování.

4.1.3 Právo na přenositelnost

Právo na přenositelnost představuje právo subjektu údajů získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, a to v případě, že zpracování osobních údajů je založeno na souhlasu nebo na smlouvě a zpracování se provádí elektronicky (kumulativní podmínky).
Při výkonu svého práva na přenositelnost má žadatel – subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.
Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.

4.1.4 Právo na opravu nebo doplnění

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů.
Pokud se správce domnívá, že zpracovávané osobní údaje jsou přesné, informuje o tom žadatele s odůvodněním.
Praktické dopady na činnost. Toto právo se samozřejmě uplatňuje již nyní v rámci vedení spisu, kdy jsou nesprávné nebo neaktuální údaje o klientech průběžně opravovány a aktualizovány. Postup je však vhodné standardizovat v interní směrnici na ochranu osobních údajů.

4.1.5 Další práva subjektů údajů

GDPR obsahuje i další práva subjektů údajů, a to právo na omezení zpracování a právo podat námitku proti automatizovanému rozhodování, přičemž tato práva budou mít pravděpodobně jen omezené uplatnění.
Ve vztahu k těmto právům odkazujeme na vzor žádosti subjektu údajů a odpovědi na žádost uvedený v příloze.

4.2. Revize smluv s dodavateli

Většina firem bude muset revidovat smlouvy se svými dodavateli a odběrateli služeb (např. poskytovatelé informatických služeb – dodavatelé software, externí účetní, daňové a auditorské společnosti,apod.).
Dodavatelé velmi často v rámci své činnosti zpracovávají osobní údaje na základě pokynů firem a jsou tedy koncovými zpracovateli osobních údajů, s nimiž musí mít firma coby správce uzavřené písemné smlouvy o zpracování osobních údajů, které obsahově vyhoví čl. 28 odst. 3 GDPR.
Firma by měla ve smlouvách se svými dodavateli – zpracovateli osobních údajů dohodnout následující:
- Specifikovat osobní údaje, které jsou zpracovávány (např. zpracování mezd zaměstnanců)
- Uvést účel zpracování osobních údajů (např. zajišťování údržby IT systému). Tímto účelem je omezen rozsah zpracování osobních údajů dodavatelem.
- Uvést závazek zpracovatele zpracovávat osobní údaje v souladu s příslušnými právními předpisy, smlouvou nebo pokyny vydanými v souladu s příslušnými právními předpisy. Nebude-li dodavatel moci z jakýchkoli

důvodů zajistit dodržování zákonných povinností či pokyny, zavazuje se o tom firmu neprodleně informovat.
- Uvést povinnost dodavatele a) zpracovávat pouze osobní údaje odpovídající stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu, b) nesdružovat osobní údaje, které byly získány k rozdílným účelům či c) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování.
- Uvést povinnost dodavatele přijmout před zpracováním osobních údajů odpovídající organizační a technická bezpečnostní opatření pro zajištění ochrany osobních údajů. Tato opatření zahrnují pro malé firmy přinejmenším zabezpečený přístup do prostor, v nichž probíhá zpracování osobních údajů, přístup k osobním údajům jen pro vybrané pracovníky dodavatele, kteří tento přístup potřebují pro účely plnění smlouvy, aj.
- Uvést závazek dodavatele proškolit své zaměstnance a další případné zástupce, kteří zpracovávají osobní údaje, o jejich povinnosti (trvající i po skončení zaměstnání nebo příslušných prací) zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.
- Uvést závazek dodavatele neprodleně oznamovat firmě veškeré případy náhodného nebo neoprávněného přístupu k osobním údajům.
Lze doporučit, aby firma vybírala své dodavatele také podle toho, jak dokáží plnit povinnosti ochrany osobních údajů podle GDPR.

4.3 Pověřenec pro ochranu osobních údajů (DPO)

GDPR zavádí pro některé správce a zpracovatele osobních údajů povinnost ustavit a obsadit funkci tzv. pověřence pro ochranu osobních údajů (DPO), který plní funkci koordinátora a supervizora ochrany osobních údajů. GDPR uvádí několik charakteristických situací, kdy správci nebo zpracovatelé jsou povinni jmenovat DPO, v čl. 37.5
Pro malé firmy bude povinné jmenování DPO spíše výjimkou. Bude to na základě následující podmínky GDPR:
Spočívají Vaše hlavní činnosti v rozsáhlém zpracování zvláštních kategorií osobních údajů.

Zvláštní kategorie osobních údajů jsou zejména údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické údaje a biometrické údaje a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.
Měřítka toho, kdy je zpracování osobních údajů rozsáhlé, GDPR nestanoví a ani ve výkladové praxi nejsou zatím nijak ustálena, a budou se dále upřesňovat.

K výše uvedenému je třeba dodat, že soulad postupů a procesů s GDPR v rámci činnosti správce není odpovědností DPO, nýbrž je povinností a odpovědností správce, resp. zpracovatele osobních údajů.
DPO nesmí určovat nebo závazně schvalovat účely nebo prostředky zpracování osobních údajů. V takovém případě může činnost DPO směřovat ke kontrole vlastní činnosti, čímž dochází k výraznému střetu zájmů. Správce je proto vždy povinen zajistit, aby byla agenda (administrativní činnosti) související s vyřizováním záležitostí regulovaných GDPR vedena v souladu se standardizovaným postupem a související odpovědnost byla svěřena konkrétní osobě odlišné od DPO.

4.4. Souhlasy subjektů údajů se zpracováním osobních údajů

Firma bude ve své praxi využívat souhlasy subjektů údajů se zpracováním jejich osobních údajů spíše omezeně, protože většina zpracování osobních údajů probíhá na základě jiných právních důvodů – zejména jako plnění ze smlouvy a plnění zákonných povinností. Příkladem toho, kdy firma zpracovává osobní údaje na základě souhlasu, může být situace, kdy by firma chtěla oslovovat veřejnost informacemi z určité zájmové oblasti, jíž se soustavně věnuje (rozesílka newsletterů splňující standardy reklamy na činnost firmy apod.). V takovém případě musí firma nejdříve získat souhlas spotřebitele – potenciálního klienta se zasláním příslušného sdělení.
Žádost o souhlas musí být konkrétně formulována a musí být doprovázena informacemi o účelu a prostředcích zpracování osobních údajů, o tom, s kým budou osobní údaje sdíleny, jak budou zabezpečeny a jaká práva má klient ve vztahu k svým údajům.
Souhlas může subjekt údajů kdykoliv odvolat. Souhlasy je nutné interně evidovat, přičemž tato evidence

musí být systematická a přehledná (s vyznačením doby, po kterou jsou osobní údaje na základě souhlasu zpracovávány). Z tohoto důvodu se doporučuje zpracování založené na souhlasu subjektů údajů využívat minimálně.

4.5. Hlášení bezpečnostních incidentů

GDPR klade velký důraz na systematickou ochranu a zabezpečení osobních údajů. GDPR zavádí povinnost jednak hlásit bezpečnostní incidenty ÚOOÚ, a v případě, že hrozí rizika pro práva a svobody dotčených subjektů údajů, také tyto incidenty neprodleně oznamovat těmto subjektům údajů.
Nařízení GDPR definuje bezpečnostní incidenty jako případy porušení zabezpečení osobních údajů, tedy velmi široce. Spadají sem nejenom přímé útoky na zpracovávaná data zvenčí anebo zevnitř (ať již úmyslné, jako je „vynesení" informací, anebo nedbalostní, jako je např. smazání části spisu v IT systému), ale i celá řada drobnějších a méně nápadných situací, kdy firma ztratí kontrolu nad daty, která spravuje – např. i ztráta nezabezpečeného mobilního telefonu s kontakty na klienty anebo notebooku se spisovým materiálem.
Hlášení bezpečnostních incidentů je povinné vždy, ledaže je nepravděpodobné, že by konkrétní porušení bezpečnosti mělo za následek riziko pro práva a svobody fyzických osob (např. ztráta zaheslovaného mobilního telefonu anebo krádež notebooku, jehož disk je standardně šifrován).
Bohužel prozatím není k dispozici přesnější vodítko k určení, které případy se musí ÚOOÚ hlásit, a které ne. Vždy je proto vhodné provést předběžné posouzení existujícího nebo potenciálního rizika a vyhodnotit jeho závažnost pro práva a svobody fyzických osob.
Jako příklad velmi závažného porušení bezpečnosti zpracovávaných osobních údajů je možné uvést ztrátu klientských spisů (ve fyzické i elektronické podobě) nebo zjištěný neoprávněný přístup ke klientským osobním údajům, které firma zpracovává. Takovéto bezpečnostní incidenty bude potřeba ohlásit ÚOOÚ i dotčeným subjektům údajů.
Přestože ne každé porušení zabezpečení bude nutné hlásit dozorovému úřadu anebo subjektu údajů, je potřeba jej vždy zaznamenat do evidence takovýchto porušení, kterou musí mít každý správce osobních údajů.
Každá firma by měla mít jako součást Směrnice vypracovaný postup řešení bezpečnostních incidentů. Tento postup zahrnuje nejen neprodlené hodnocení incidentu a jeho ohlášení ÚOOÚ a případně dotčeným subjektům údajů, ale také co nejrychlejší řešení incidentu a přijetí opatření k tomu, aby se pokud možno podobný bezpečnostní incident nemohl opakovat.

5. PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

Při předávání osobních údajů do zahraničí do zemí mimo EU je třeba postupovat podle předepsaných postupů v GDPR. V podstatě platí následující doporučení:
- Předávání zahrnuje nejen aktivní komunikaci osobních údajů, ale rovněž jejich zpřístupnění, např. formou přístupových práv k databázi.
- Pokud je předávání osobních údajů v rámci EU anebo EHP, nemusí se provádět žádné zvláštní postupy a data lze předat stejně, jako by se jednalo o předání v rámci ČR.
- Pokud jde o předání mimo EU, je třeba zkontrolovat, zda se jedná o zemi, která dle rozhodnutí Evropské komise poskytuje dostatečnou ochranu osobních údajů, a tam platí stejný režim jako pro předání v rámci EU. Mezi takové státy patřily Faerské ostrovy, Jersey, Ostrov Man, Guermsey, Argentina, Švýcarsko, Uruguayská republika, Andorra a Nový Zéland.
U několika dalších států, např. Izrael, Kanada nebo USA platí zvláštní režim – více informací lze nalézt na webových stránkách ÚOOÚ.
- Pokud jsou osobní údaje předávány do jiných než výše uvedených zemí, lze využít tzv. standardních smluvních doložek přijatých Evropskou komisí. Jde o předepsanou textaci smluvních ustanovení mezi správcem/zpracovatelem ze země EU a správcem/zpracovatelem mimo EU. Při použití těchto předepsaných smluvních ustanovení není nutné žádat o souhlas
ÚOOÚ s přenosem dat do zahraničí; texty všech standardních smluvních doložek jsou k dispozici na webu ÚOOÚ.
Navíc k výše uvedeným možnostem postupu existují další možnosti, které jsou podrobně popsány na webu ÚOOÚ

6. POSTUP PŘI KONTROLE ÚOOÚ

ÚOOÚ jakožto dozorový úřad má dle čl. 58 odst. 1 písm. a) GDPR pravomoc nařídit správcům a zpracovatelům zpřístupnění všech informací nezbytných pro výkon kontrolní činnosti.
Kontrola ÚOOÚ by měla být především zaměřena na ověření toho, zda kontrolovaná firma:
- plní informační povinnosti vůči subjektům údajů, jejichž data zpracovává;
- pořídila a udržuje povinnou dokumentaci (zejména záznamy o činnostech zpracování dle čl. 30 a dokumentaci prokazující naplnění zásad zpracování a ochrany osobních údajů dle čl. 5, 6, 25 a 32 GDPR);
- umožňuje hladký výkon práv subjektů údajů (s přihlédnutím k výše popsaným omezením);
- přijala odpovídající bezpečnostní opatření k zajištění bezpečnosti zpracovávaných osobních údajů;
- má přehledný systém evidence zpracovávaných osobních údajů.

Výše uvedené by měla být každá firma schopna doložit.
Otevřenou otázkou zůstává národní legislativa a následná aplikační praxe ÚOOÚ a soudů. Ustanovení § 56 odst. 1 a 2 vládního návrhu zákona o zpracování osobních údajů opravňuje ÚOOÚ se seznamovat se všemi informacemi nezbytnými pro plnění konkrétního úkolu, což platí i pro informace chráněné povinností mlčenlivosti podle jiného právního předpisu.
Oznámení o chystané kontrole z ÚOOÚ by mělo obsahovat informace o tom, jaké dokumenty ÚOOÚ požaduje ke kontrole připravit. Doporučujeme zvážit, zda je čas mezi doručením oznámení a datem kontroly dostatečný pro přípravu na kontrolu.
Pokud potřebujete víc času, doporučujeme požádat ÚOOÚ o delší čas na přípravu.
Kontroloři v některých případech požadují kopie dokumentů, aby je mohli prověřit mimo firmu. Vždy je třeba pořídit podrobný seznam předaných kopií a nechat si jej potvrdit od kontrolora.
Z každého jednání s kontrolory doporučujeme si vyžádat zápis.