**METODIKA PRO PODNIKATELSKÉ**

**SUBJEKTY K DOSAŽENÍ SHODY S GDPR**

**Obsah:**

1. ÚVOD

2. POJMY

3. MINIMÁLNÍ POŽADAVKY NA SHODU PONIKATELE S GDPR

4. ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PODLE GDPR

5. SOUHLAS SE ZPRACOVÁNÍM OÚ.

6. ZÁKLADNÍ VZOROVÁ INTERNÍ SMĚRNICE O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

 6.1 Záznamy o činnostech zpracování

 6.2 Vyřizování žádostí a stížností subjektů údajů

 6.3 Revize smluv s dodavateli

 6.4 Pověřenec pro ochranu osobních údajů (DPO)

 6.5 Souhlasy subjektů údajů se zpracováním osobních údajů

 6.6 Hlášení bezpečnostních incidentů

7. PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

**1. ÚVOD**

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 (obecné nařízení o ochraně osobních údajů; dále jen jako „GDPR“), které nabývá účinnosti 25. května 2018, představuje základní stavební kámen v novém evropském legislativním rámci ochrany osobních údajů a rovněž první milník v chápání ochrany osobních údajů jako základního regulačního nástroje pro oblast tzv. digitální ekonomiky v EU. Do působnosti GDPR spadá veškeré zpracování osobních údajů fyzických osob na území EU/EHP, a to bez ohledu na formu účel, cíl, právní titul, formu zpracování (automatizované/elektronické i manuální) anebo postavení osoby, která za zpracování osobních údajů odpovídá. Přes pochopitelné odborné diskuse o tom, v jakém rozsahu se GDPR má vztahovat na povolání s garantovanou povinností mlčenlivosti (notáři, advokáti, daňoví poradci, dále též lékaři a poskytovatelé pečovatelských služeb, kněžská povolání ad.), je již nyní zřejmé, že GDPR se dotkne všech profesí v podnikatelské sféře, neboť k výměně osobních údajů bude docházet i v běžném obchodním styku ( obchodník versus obchodník a obchodník versus spotřebitel/klient).

**2. POJMY**

Základními pojmy GDPR jsou:

- **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, 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.

- **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](http://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, nebo

b) zpracování OÚ není příležitostné,

dotkne se tato povinnost prakticky každého podnikatelského subjektu.

- **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 (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. Každý podnikatelský subjekt bude muset zpracovat analýzu rizik ve vztahu ke zpracování osobních údajů, která provádí. Blíže o analýze rizik viz vzor sestavy pro analýzu rizik v příloze této Metodiky.

- **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. Blíže o hlášení bezpečnostních incidentů viz část 6.6 této Metodiky.

**3. MINIMÁLNÍ POŽADAVKY NA SHODU PODNIKATELE S GDPR**

Vzhledem k obsahu činnosti a s tím související nutnosti evidovat osobní údaje je nezbytné, aby došlo k naplnění přinejmenším požadavků minimální shody podnikatele 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 v podmínkách podnikatelských subjektů 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). Blíže viz část 6.1 této Metodiky. Pakliže takovou dokumentaci nepořídí podnikatelský subjekt ve spolupráci s dodavatelem informačních technologií, mohou být vhodnými podkladovými materiály pro vypracování této dokumentace odborná literatura v oblasti bezpečnosti informací, kybernetické bezpečnosti, případně zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, resp. příloha č. 4 k jeho prováděcí vyhlášce č. 316/2014 Sb.

**4. ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PODLE GDPR**

Celé GDPR vychází z několika obecných zásad zpracování a ochrany osobních údajů (obsažených především v čl. 5, 6, 25 a 32 GDPR, dále ze zásady přístupu založeného na řízení rizik a informačního sebeurčení subjektů 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), 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.

**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. 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.

**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 v databázi aktualizována

**Zásada omezeného uložení** znamená povinnost uchovávat osobní údaje jen po dobu nezbytně nutnou k naplnění účelu zpracování.

**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 představují 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. 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.

**5. SOUHLAS SE ZPRACOVÁNÍM OÚ**

Podnikatelské subjekty budou ve své praxi využívat písemné souhlasy subjektů údajů se zpracováním jejich osobních údajů. Aby bylo možno považovat souhlas, udělený subjektem údajů, za platný, musí splňovat nároky na jeho svobodnost, konkrétnost, informovanost a jednoznačnost. Dále musí být možné jednou udělený souhlas odvolat, a to způsobem, ne složitějším, než jakým byl souhlas udělen.

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.

**6. ZÁKLADNÍ VZOROVÁ INTERNÍ SMĚRNICE O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ**

Cílem této části Metodiky je připravit ve snadno srozumitelné formě základ interní směrnice, popisující postupy ochrany zpracovávaných osobních údajů při podnikatelské činnosti (dále jen „Vzorová směrnice“). Směrnice na ochranu osobních údajů je jedním ze základních dokumentů ve vztahu k ochraně osobních údajů. Směrnice by měla obsahovat tyto údaje:

* zásady zpracování osobních údajů,
* hiearchii odpovědnosti za ochranu osobních údajů ve společnosti,
* postupy a procesy pro nakládání s osobními údaji,
* postupy pro realizaci práv subjektů údajů,
* systém zajištění povědomí o ochraně osobních údajů ve společnosti,
* postupy pro mimopodnikovou komunikaci

Vzorová směrnice má následující části:

**6.1 Záznamy o činnostech zpracování**

Kategorie a charakteristiky zpracování osobních údajů

Komentáře pro vyplnění

1. Jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů [článek 30 odst. 1 písm. a) GDPR]:

Uveďte jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů.

Kategorie a charakteristiky zpracování osobních údajů

Komentáře pro vyplnění

2. Identifikace příslušných zpracování osobních údajů [článek 30 odst. 1 písm. b) GDPR]:

Uveďte seznam všech zpracování osobních údajů, které provádíte, podle hlavních kategorií:

(i) zaměstnanci;

(ii) odběratelé;

(iii) dodavatelé;

(iv) ostatní.

3. Proč (za jakým účelem) a na základě jakého právního titulu se osobní údaje v rámci zpracovávání zpracovávají [článek 30 odst. 1 písm. b) GDPR]?

Uveďte pro každé zpracování osobních údajů účel (cíl, smysl zpracování) a rovněž právní titul zpracování (půjde zejména o plnění smlouvy se subjektem a plnění zákonných povinností).

4. Jaké osobní údaje jsou zpracovávány v rámci zpracování [článek 30 odst. 1 písm. c) GDPR]?

Pro každé zpracování uveďte všechny kategorie osobních údajů, které zpracováváte.

5. Z jakých zdrojů jsou osobní údaje získány [(článek 30 odst. 1 písm. c) GDPR]?

Uveďte všechny subjekty, od nichž získáváte osobní údaje, které v rámci své činnosti zpracováváte.

6. Kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích:

Uveďte všechny kategorie osob a organizací, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích.

7. V jakém termínu a jak se osobní údaje likvidují [článek 30 odst. 1 písm. f) GDPR]?

Uveďte pro každé zpracování osobních údajů archivační a skartační lhůtu. Je-li ve společnosti archivační/skartační řád vydán a naplňován, lze odkázat na příslušný interní předpis.

8. Jakým způsobem se osobní údaje aktualizují [článek 30 odst. 1 písm. g) GDPR]?

Uveďte způsob aktualizace osobních údajů – viz zásada přesnosti v části 4.

9. Které listinné a elektronické evidence (spisovny, archivy, IT systémy, datová úložiště) provádějí zpracování [článek 30 odst. 1 písm. g) GDPR]?

Uveďte podrobně, jaké listinné evidence a IT systémy využíváte pro svou činnost a jejich vazbu na konkrétní zpracování (tzn. které evidence/IT systémy provádějí jaké zpracování osobních údajů).

Kategorie a charakteristiky zpracování osobních údajů

10. Je prostředí ve společnosti pravidelně bezpečnostně testováno (zejm. IT systémy)? Interně nebo externími konzultanty? [článek 30 odst. 1 písm. g) GDPR].

GDPR klade velký důraz na bezpečnost zpracování osobních údajů. Vaše IT systémy by měly být bezpečnostně testovány – interně nebo externě. V závislosti na objemu zpracovávaných osobních údajů je třeba zvolit délku časového období mezi dvěma testy.

11. Jak je zajištěna bezpečnost šifrování dat při klientské komunikaci [článek 30 odst. 1 písm.

g) GDPR]?

Uveďte, jak řešíte komunikaci citlivých klientských informací a dále např. jak zabezpečujete předání údajů o zaměstnancích externí účetní firmě.

12. Jak je zajištěna bezpečnost sdílení dat s externími subjekty? Mají všichni externí dodavatelé, zpracovávající osobní údaje, uzavřené smlouvy o zpracování osobních údajů, poskytující odpovídající záruky ochrany [článek 30 odst. 1 písm. g) ve spojení s článkem 28 GDPR]?

Uveďte, zda vaši dodavatelé, kteří mohou mít přístup ke zpracovávaným osobním údajům (např. účetní agentura nebo firma spravující váš webový systém,) mají uzavřeny smlouvy o zpracování osobních údajů.

13. Je zajištěna nevratná likvidace dat v rámci databázového systému [článek 30 odst. 1 písm. g) GDPR]?

Uveďte, zda na konci životního cyklu příslušného zpracování osobních údajů je váš IT systém schopný nevratně osobní údaje vymazat.

14. Je k dispozici procedura k určení práv subjektů údajů a jejich výkon s ohledem na jejich data, která jsou zpracovávána v rámci zpracování?

Uveďte, zda máte zaveden interní proces vyřizování žádostí subjektů údajů ve vztahu k právům subjektů údajů – viz část 6.2 níže, a jakou formou postupujete (např. odkaz na formuláře na vašem webu nebo v listinné podobě). Rovněž je potřeba vymezit, v jakých situacích jsou práva subjektů omezována a z jakých titulů. ( např. dohody o mlčenlivosti a utajení)

15. Poskytují se oprávněným subjektům údajů předepsané informace, zejména o:

- rozsahu a účelu zpracování,

- způsobu zpracování osobních dat, komu mohou být osobní údaje zpřístupněny?

Uveďte, kde a jakou formou poskytujete předepsané informace pro subjekty údajů.

16. Zabraňují nasazené technické prostředky a uplatňovaná organizační opatření nahodilému anebo neoprávněnému přístupu k osobním údajům, jejich změně, zcizení, zneužití, zničení nebo ztrátě [článek 30 odst. 1 písm. g) GDPR]?

Uveďte, jaká bezpečnostní opatření používáte pro zajištění bezpečnosti zpracovávaných osobních údajů (provozní opatření, IT opatření). Je možno odkázat na interní předpis.

17. Jsou zpracovávané osobní údaje přenášeny do zahraničí nebo jsou přístupné ze zahraničí [článek 30 odst. 1 písm. e) GDPR]?

Uveďte, zda jsou vámi zpracovávané osobní údaje přenášeny do zahraničí nebo přístupné ze zahraničí. Více viz část 7 níže.

18. Jsou pracovníci, mající přístup k osobním údajům v rámci zpracování osobních údajů, proškoleni? Mají tito pracovníci ve svých smlouvách sjednánu povinnost mlčenlivosti ve vztahu ke zpracovávaným osobním údajům [článek 30 odst. 1 písm. g) GDPR]?

Uveďte, zda jsou pracovníci vaší společnosti proškoleni o GDPR a zásadách ochrany osobních údajů. a o uzavřených dohodách o mlčenlivosti.

**6.2 Vyřizování žádostí a stížností subjektů údajů**

GDPR obsahuje řadu práv subjektů údajů. Podnikatelské subjekty musejí 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 toto doloručení: doporučení:

- Podnikatelské subjekty musejí 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 společnosti

**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. Níže jsou uvedeny stručné informace o jednotlivých právech. V příloze jako jeden ze vzorů uvádíme vzor žádosti a odpovědi na žádost.

**6.2.1 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.

**6.2.2 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 nebo výkon právních nároků;

b) pro výkon práva na svobodu projevu a informace;

c) pro splnění 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.

**6.2.3 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.

**6.2.4 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.

**6.2.5 Další práva subjektů údajů**

GDPR obsahuje i další práva subjektů údajů, a to právo na omezení zpracování a právo podat námitku proti automatizovanému rozhodování.

.

**6.3 Revize smluv s dodavateli**

Většina podnikatelských subjektů bude muset revidovat smlouvy se svými dodavateli a odběrateli, (např. poskytovatelé informatických služeb – dodavatelé software, externí účetní, daňové a auditorské společnosti, poskytovatelé právních služeb, vymáhací agentury apod.). Vzor základní smlouvy o zpracování osobních údajů tvoří přílohu této Metodiky.

Podnikatelské subjekty by měly ve smlouvách se svými dodavateli – zpracovateli osobních údajů dohodnout následující:

- Specifikovat osobní údaje, které jsou zpracovávány.

- Uvést účel zpracování osobních údajů. Tímto účelem je omezen rozsah zpracování osobních údajů dodavatelem.

- Uvést závazek zpracovatele zpracovávat osobní údaje v souladu s příslušnými právními předpisy, smlouvou nebo pokyny podnikatelského subjektu, vydanými v souladu s příslušnými právními předpisy. Nebude-li dodavatel moci z jakýchkoli důvodů zajistit dodržování zákonných povinností či pokyny zadavatele, zavazuje se o tom podnikatelský subjekt 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 podnikatelské subjekty 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 podnikatelskému subjektu veškeré případy náhodného nebo neoprávněného přístupu k osobním údajům.

**6.4 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 GDPR.

 Povinnost funkci DPO ustavit vzniká u správců a zpracovatelů, u kterých lze předpokládat vyšší pravděpodobnost výskytu nestandardních jevů při zpracování osobních údajů (např. z důvodu rozsahu anebo citlivosti údajů). Ostatní správci a zpracovatelé mohou funkci ustavit dobrovolně.

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.

**6.5 Souhlasy subjektů údajů se zpracováním osobních údajů**

Žádost o souhlas se zpracováním osobních údajů 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.

**6.6 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 podnikatelský subjekt ztratí kontrolu nad daty, která spravuje – např. i ztráta nezabezpečeného mobilního telefonu s kontakty na zaměstnance a obchodní partnery 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.

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.

Každý podnikatelský subjekt by měl 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.

**7. 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. K 6. 3. 2018 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.

V Ústí nad Orlicí dne 25.5.2018

**Přílohy:**

1. **Vzorová směrnice pro ochranu osobních údajů**
2. **Příloha č. 1 ke směrnici pro ochranu OÚ**
3. **Informační doložka do smluv**
4. **Informační doložka – dodatek**
5. **Vzor souhlasu se zpracováním osobních údajů**
6. **Privacy policy**