



GDPR - základní pojmy

ESO9 international a.s.
U Mlýna 2305/22, 141 Praha 4 – Záběhlice
tel.: +420 228 809 000
e-mail: info@eso9.cz
www.eso9.cz

Zpracoval: Zavadilová Marcela
Dne: 27.11.2017

Revize:
Dne: 5.3.2018

Obsah

1.	ZÁKLADNÍ INFORMACE O OBECNÉM NAŘÍZENÍ	4
2.	NEJDŮLEŽITĚJŠÍ POJMY Z OBECNÉHO NAŘÍZENÍ (ČL. 4).....	4
	OSOBNÍ ÚDAJ	4
	ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ – CITLIVÉ ÚDAJE	4
	SUBJEKT ÚDAJŮ	4
	ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ	4
	PROFILOVÁNÍ	5
	SPRÁVCE	5
	ZPRACOVATEL	5
3.	ZÁKLADNÍ ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ	5
3.1	ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ (ČL. 5).....	5
	Zásada zákonnosti (čl. 6)	6
	Zásada korektnosti a zásada transparentnosti	6
	Zásada omezení účelu.....	6
	Minimalizace údajů	7
	Zásada přesnosti	7
	Zásada omezení uložení	7
	Zásada integrity a důvěrnosti	7
4.	PRÁVA SUBJEKTŮ OSOBNÍCH ÚDAJŮ	7
4.1	OBECNÉ POSTUPY PRO VÝKON PRÁV SUBJEKTU ÚDAJŮ (ČL. 12)	7
	Právo na informace (čl. 13, 14).....	8
	Právo na přístup k osobním údajům (čl. 15)	9
	Právo na opravu a doplnění (čl. 16)	9
	Právo na výmaz - „být zapomenut“ (čl. 17)	10
	Právo na omezení zpracování (čl. 18).....	10
	Právo na přenositelnost údajů (čl. 20)	10
	Právo vznést námitku (čl. 21).....	11
	Právo nebýt předmětem automatizovaného individuálního rozhodování (čl. 22)	11
	Omezení práv a zásad zpracování (čl. 23).....	11
5.	POVINNOSTI SPRÁVCŮ OSOBNÍCH ÚDAJŮ.....	11
5.1	POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ (ODDÍL 4)	11
5.2	POVINNOST VÉST ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ (ČL. 30)	12
5.3	OHLAŠOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ (ČL. 33)	12
6.	VZTAH SPRÁVCE A ZPRACOVATELE OSOBNÍCH ÚDAJŮ	13
6.1	SPRÁVCE A ZPRACOVATEL OSOBNÍCH ÚDAJŮ.....	13
6.2	VZTAH SPRÁVCE A ZPRACOVATELE (ČL. 28).....	13
	Smlouva.....	14
6.3	ŘETĚŽENÍ ZPRACOVATELŮ.....	14
7.	PROSAZOVÁNÍ OBECNÉHO NAŘÍZENÍ A SANKCE ZA JEHO NEDODRŽOVÁNÍ.....	14

7.1	DOZOROVÝ ÚŘAD (ČL.51).....	14
7.2	SANKCE A UKLÁDÁNÍ POKUT (ČL. 83, 84).....	15
8.	ZÁVĚR.....	15

1. Základní informace o Obecném nařízení

Celý oficiální název česky:

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)

Běžně se používá zkrácený název **Obecné nařízení o ochraně osobních údajů**, **Obecné nařízení** nebo jen **Nařízení**. Z anglického oficiálního názvu **General Data Protection Regulation** vznikla velmi často používaná zkratka **GDPR**.

Nařízení je již platné, od **25. května 2018 bude použitelné** a nahradí Směrnicí 95/46/ES a zákon 101/2000 Sb., o ochraně osobních údajů. **Nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.**

Jednotlivé členské státy EU mají možnost upravit si některé věci obsažené v Obecném nařízení zákonem (jedná se však jen o drobné úpravy jako je např. věk dítěte pro souhlas se zpracováním osobních údajů, stanovení dozorového úřadu atd.). V ČR je již připraven návrh zákona o zpracování osobních údajů, který v současné době čeká na projednání vládou, žádné podstatné změny oproti Obecnému nařízení však nepřinese.

2. Nejdůležitější pojmy z Obecného nařízení (čl. 4)

Osobní údaj

Osobním údajem je každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, a to zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Zvláštní kategorie osobních údajů – citlivé údaje

Jedná se o přesně danou skupinu osobních údajů uvedených v čl. 9 Obecného nařízení. Za zvláštní kategorie os. údajů jsou považovány osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuální životě nebo sexuální orientaci fyzické osoby.

Pro zpracování zvláštních kategorií os. údajů stanoví Obecné nařízení přísnější pravidla, právní důvody zpracování zvláštních kategorií os. údajů stanovuje čl. 9 Obecného nařízení.

Pokud hlavní činnost správce spočívá v rozsáhlém zpracování zvláštních kategorií os. údajů, musí stanovit pověření.

Subjekt údajů

Subjektem údajů je fyzická osoba, již se osobní údaje týkají. Subjekt údajů není právnická osoba. Údaje vztahující se k právnické osobě tak nejsou osobními údaji. Osobní údaje mohou být pouze ve vztahu k žijící fyzické osobě, jelikož Obecné nařízení vylučuje svoji působnost na údaje o zesnulých osobách.

Zpracování osobních údajů

Zpracováním je jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Zpracování ve smyslu Obecného nařízení však nelze chápat jako jakékoli nakládání s osobním údajem. Zpracování osobních údajů je nutné považovat již za sofistikovanější činnost, kterou správce s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky.

Profilování

Jde o formu automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází nebo pohybu.

Byť je profilování nově definováno, nejde de facto o žádnou novinku, jelikož k profilování dochází i v současné době. Profilování není a priori Obecným nařízením zakázáno. Je však důležité, aby se dělo v předvídaných případech a na základě stanovených pravidel. Profilování je běžné např. ve finančních službách, kdy finanční subjekty profilují např. klienta žádajícího o hypotéku, u kterého hodnotí schopnost splácet.

Správce

Správce je subjekt, nerozhoduje jaké právní formy, který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně zodpovídá. Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti (např. zákonem stanovené povinnosti, ze smluv), ale může je zpracovávat i pro vlastní určené účely, např. pro své oprávněné zájmy, pokud tyto zájmy nepřevyšují zájem na ochraně základních práv a svobod fyzických osob.

Správce může být jakýkoli subjekt. Správce může být i fyzická osoba, pokud zpracovává osobní údaje způsobem, že tento způsob již vylučuje uplatnění výjimky pro osobní či domácí činnosti.

Zpracovatel

Zpracovatelem je subjekt, kterého si správce najímá, aby pro něj prováděl s osobními údaji zpracovatelské operace. Jinými slovy zpracovatel zpracovává osobní údaje pro správce. Od správce se zpracovatel liší tím, že v rámci činnosti pro správce může provádět jen takové zpracovatelské operace, kterými jej správce pověřil nebo které vyplývají z činnosti, pro kterou byl zpracovatel správcem pověřen. Je nutné poznamenat, že zpracovatel je zpracovatelem pouze ve vztahu k osobním údajům poskytnutým správcem, nikoli k osobním údajům, které zpracovává pro účely, které se jej přímo dotýkají (např. je správcem při zpracování osobních údajů vlastních zaměstnanců).

Stejně jako u správce, ani u zpracovatele není určující jeho právní forma.

3. Základní zásady ochrany osobních údajů

Obecné nařízení oproti aktuálně platným zákonům přináší dva nové přístupy k ochraně osobních dat. Těmi jsou princip **odpovědnosti správce osobních údajů** a **přístup založený na riziku**.

Princip odpovědnosti znamená především **odpovědnost správce za dodržení zásad zpracování**, které jsou zakotveny v obecném nařízení.

Přístup založený na riziku znamená, že **správce již od počátku zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext a účel zpracování a přihlídnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu musí přizpůsobit i zabezpečení osobních údajů**.

3.1 Zásady zpracování osobních údajů (čl. 5)

Obecné nařízení nově přináší **princip zodpovědnosti** - **správce zodpovídá** za dodržení všech **zásad zpracování** osobních údajů uvedených v Obecném nařízení a musí být schopen soulad zpracování doložit.

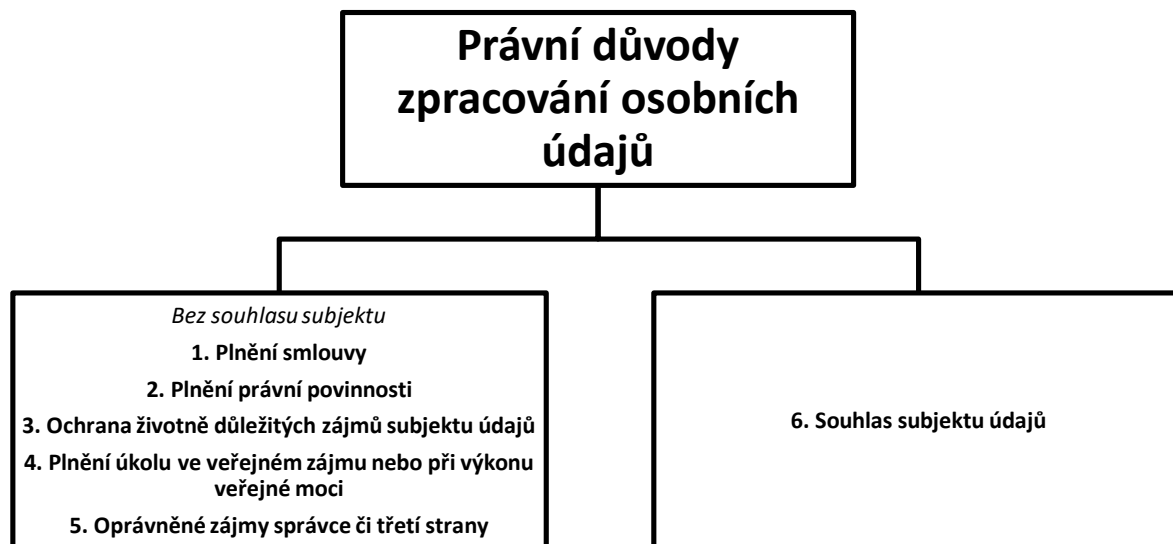
Zásady zpracování podle čl. 5 odst. 1 Obecného nařízení jsou:

- **Zákonnost**
- **Korektnost a transparentnost**
- **Omezení účelu**
- **Minimalizace údajů**
- **Přesnost**
- **Omezení uložení**
- **Integrita a důvěrnost**

Zásada zákonnosti (čl. 6)

Správce může osobní údaje zpracovávat k určitému účelu (a tedy vůbec je mít) pouze tehdy, má-li k takovému zpracování alespoň jeden **právní důvod**. Právních důvodů zpracování může být více, pokud pominou, musí správce osobní údaje zlikvidovat. Většinou ale nějaký důvod zůstává, i když ne pro všechny údaje.

Právní důvody zpracování uvádí Obecné nařízení v čl. 6. Všeobecně rozšířený názor, že pro zpracování osobních údajů je nutný souhlas subjektu údajů, není úplně správný. Souhlas je pouze jedním z právních důvodů zpracování a měl by být volen až jako poslední možnost, protože je lehce odvolatelný.



Zásada korektnosti a zásada transparentnosti

Správce nesmí subjektu os. údajů **zastírat účel, pro který jsou os. údaje zpracovávány**. Zároveň by měl subjektu údajů poskytnout informace zejména o tom, kdo, jakým způsobem a v jakém rozsahu os. údaje zpracovává a komu jsou os. údaje předávány. Informace o zpracování musí být snadno přístupné a srozumitelné. Více viz práva subjektů osobních údajů.

Zásada omezení účelu

Os. údaje musí být shromažďovány **pro určité, výslovně vyjádřené legitimní účely** a nesmějí být zpracovávány způsobem, který je s těmito účely neslučitelný. Zpracovávat lze pouze os. údaje, které jsou nezbytné pro konkrétní účel.

Minimalizace údajů

Zpracovávat lze pouze osobní údaje **přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu ke stanovenému účelu zpracování**. Nelze požadovat po subjektu os. údajů více údajů, než je nezbytně nutné.

Správce má povinnost zavést vhodná technická a organizační opatření k zajištění toho, aby se zpracovávaly jen os. údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné – týká se to množství, rozsahu zpracování, doby uložení a dostupnosti os. údajů.

Zásada přesnosti

Osobní údaje musí být zpracovávány **v přesné podobě** a v případě potřeby **musí být** aktualizované. Správce nemusí aktivně vyhledávat nepřesné údaje, musí však vyhovět subjektu os. údajů při žádosti o aktualizaci.

Zásada omezení uložení

Os. údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů po dobu ne delší, než je nezbytně nutné pro účely, pro které jsou zpracovávány. Jde o povinnost **zlikvidovat os. údaje, pokud pomine účel zpracování**. Likvidaci lze provést i anonymizací dat. Zásada souvisí s právem subjektu os. údajů na výmaz.

Zásada integrity a důvěrnosti

Zpracovávané os. údaje by měly být dostatečně zabezpečeny, a to prostřednictvím vhodných technických nebo organizačních opatření chránících je před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Jde o vyjádření požadavku na zajištění důvěrnosti a integrity systému, ve kterém se os. údaje zpracovávají.

4. Práva subjektů osobních údajů

Práva subjektů osobních údajů tvoří nedílnou součást ochrany osobních údajů při jejich zpracování. Vztah mezi správcem a subjektem osobních údajů je většinou nerovný, subjekt osobních údajů musí často zpracování osobních údajů strpět. Zajištění řádného výkonu práv subjektu údajů je nezbytnou podmínkou pro soulad zpracování jako celku s Obecným nařízením.

Pokud nebyl v organizaci jmenován pověřenec pro ochranu osobních údajů, lze doporučit pověřit určitou osobu, aby se přiměřeným způsobem věnovala ochraně osobních údajů, včetně reagování správce na požadavek výkonu práv ze strany subjektu údajů.

4.1 Obecné postupy pro výkon práv subjektu údajů (čl. 12)

Obecně musí dle čl. 12 Obecného nařízení správce osobních údajů informovat či provádět výkon práv subjektu osobních údajů **stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků**. Informace se poskytují písemně nebo jinými vhodnými prostředky, včetně elektronické formy, a vyloučeno není ani ústní sdělení, pokud o to subjekt osobních údajů požádá. Typické pro správce bude zveřejňování obecných informací o zpracování na internetových stránkách.

Informace se poskytují bez zbytečného odkladu a v každém případě do 1 měsíce od obdržení žádosti. Vše se děje bezplatně. Pokud jsou žádosti subjektu osobních údajů dle správce (musí to doložit) zjevně nedůvodné nebo nepřiměřené (opakují se), může správce uložit přiměřený poplatek zohledňující administrativní náklady nebo odmítnout žádosti vyhovět.

Právo na informace (čl. 13, 14)

Právo na informace naplňuje zásadu transparentnosti zpracování osobních údajů. Jedná se o **aktivní povinnost pro správce, musí tuto povinnost plnit automaticky** a nikoliv na požádání subjektem údajů, tak jak je to u některých jiných práv.

Při jakémkoliv získávání osobních údajů musí správce poskytnout subjektu údajů základní informace o zpracování osobních údajů. Rozlišuje se obsah informací podle toho, **zda správce získal či nezískal osobních údaj přímo od subjektu osobních údajů**.

Základní poskytované minimum	Osobní údaje byly získány od subjektu údajů	Osobní údaje nebyly získány od subjektu údajů
totožnost a kontaktní údaje správce a jeho případného zástupce	ANO	ANO
kontaktní údaje případného pověřence pro ochranu osobních údajů	ANO	ANO
účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování	ANO	ANO
oprávněné zájmy správce nebo třetí strany	ANO	ANO
případné příjemce nebo kategorie příjemců osobních údajů	ANO	ANO
případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci	ANO	ANO
kategorie dotčených osobních údajů	ANO	ANO

Kromě základních informací uvedených v předchozí tabulce by měl správce osobních údajů poskytnout subjektu údajů v okamžiku získání osobních údajů další informace, pokud jsou nezbytné pro zajištění spravedlivého a transparentního zpracování:

Další informace, pokud je to nezbytné pro zajištění spravedlivého a transparentního zpracování	Osobní údaje byly získány od subjektu údajů	Osobní údaje nebyly získány od subjektu údajů
dobu, po kterou budou osobní údaje uloženy	ANO	ANO
právo požadovat od správce přístup k osobním údajům, právo na opravu nebo výmaz, popřípadě omezení zpracování, právo vznést námitku proti zpracování a právo na přenositelnost	ANO	ANO
existence práva odvolat kdykoli souhlas	ANO	ANO
existence práva podat stížnost u dozorového úřadu	ANO	ANO
zdroj, ze kterého osobní údaje pocházejí	NE	ANO

skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem a důsledky neposkytnutí těchto údajů	ANO	NE
skutečnost, zda dochází k automatizovanému rozhodování, včetně profilování a smysluplné informace týkající se použitého postupu	ANO	ANO

Informace při získávání osobních údajů přímo od subjektu se poskytují v okamžiku jejich získání, tedy při jednání se subjektem údajů.

Pokud nebyly osobní údaje získány od subjektu osobních údajů, má správce povinnost poskytnout informace:

- v přiměřené lhůtě po získání osobních údajů, ale nejpozději do 1 měsíce;
- nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být údaje použity pro účely této komunikace;
- nejpozději při prvním zpřístupnění osobních údajů, pokud je má správce v úmyslu zpřístupnit příjemci;
- informace není nutné poskytovat, pokud subjekt údajů již uvedené informace má, nebo se ukáže, že poskytnutí takových informací by vyžadovalo nepřiměřené úsilí.

V praxi bude nutné nalézt zlatou střední cestu mezi požadavky na informování a srozumitelností a jednoduchostí informací.

Právo na přístup k osobním údajům (čl. 15)

Právo na přístup k osobním údajům je aktivním právem subjektu údajů, pro správce znamená povinnost tehdy, když subjekt údajů požádá o přístup k osobním údajům. Správce musí vydat potvrzení, zda jsou osobní údaje subjektu zpracovávány a pokud ano, umožnit přístup k těmto údajům (např. formou jejich poskytnutí) a k následujícím informacím:

- Účely zpracování
- Kategorie dotčených osobních údajů
- Příjemci nebo kategorie příjemců, kterým byly nebo budou os. údaje zpřístupněny
- Doba po kterou budou os. údaje uloženy, případně kritéria pro její stanovení
- Existence práva na opravu nebo výmaz, omezení zpracování anebo vznesení námítky proti zpracování
- Právo podat stížnost u dozorového úřadu
- Veškeré dostupné informace o zdroji os. údajů, pokud nebyly získány od subjektu údajů
- Skutečnost, zda dochází k automatizovanému rozhodování, včetně profilování, a související smysluplné informace týkající se použitého postupu.

Správce musí bezplatně poskytnout subjektu údajů kopii zpracovávaných os. údajů. Týká se i záznamů z kamerového systému či tel. rozhovoru.

Právo na opravu a doplnění (čl. 16)

Subjekt má právo na opravu nepřesných os. údajů a na doplnění neúplných os. údajů. Správce není povinen aktivně vyhledávat nepřesné údaje, je však vhodné v závislosti na kontextu a účelech zpracování např. při osobním kontaktu nebo při písemném styku požádat subjekt o aktualizaci identifikačních a kontaktních údajů.

Platí oznamovací povinnost – musíme informovat o opravě a doplnění os. údajů případné příjemce.

Právo na výmaz - „být zapomenut“ (čl. 17)

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a **správce má povinnost** (musí sám aktivně) osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
- subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, 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 zpracovány protiprávně;
- osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje;
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1 Obecného nařízení.

Uvedené důvody se podle čl. 17 odst. 3 Obecného nařízení nepoužijí, pokud je zpracování nadále nezbytné:

- pro výkon práva na svobodu projevu a informace;
- pro splnění právní povinnosti, která se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;
- z důvodů veřejného zájmu v oblasti veřejného zdraví;
- pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely;
- pro určení, výkon nebo obhajobu právních nároků.

Důležité je hlídat také mazání - likvidaci osobních údajů – skartace papírových dokumentů, anonymizace.

Platí oznamovací povinnost – musíme informovat o výmazu osobních údajů případné příjemce.

Právo na omezení zpracování (čl. 18)

Subjekt údajů má právo na to, aby správce omezil zpracování, v kterémkoli z těchto případů:

- subjekt údajů popírá přesnost osobních údajů;
- zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
- subjekt údajů vznese námitku proti zpracování, je nutné ověřit, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

Podstatným znakem omezení je dočasnost, čímž se liší od likvidace.

Platí oznamovací povinnost – musíme informovat o omezení zpracování případné příjemce.

Právo na přenositelnost údajů (čl. 20)

Subjekt údajů má právo získat osobní údaje, **jež poskytl správci a které se ho týkají, ve strukturovaném, běžně používaném a strojově čitelném formátu** a zároveň má právo předat tyto údaje jinému správci, a to i prostřednictvím původního správce v případě, že **zpracování je založeno na souhlasu subjektu údajů nebo na smlouvě** a provádí se automatizovaně.

Důležitý je **formát**, ve kterém musí být informace poskytnuty. Týká se to pouze informací, které jsou zpracovávány **na základě souhlasu nebo smlouvy**, musí jít o **automatizované zpracování** (na zpracování prováděné ručně se přenositelnost nevztahuje).

Právo vznést námitku (čl. 21)

Subjekt údajů má z důvodů týkajících se jeho konkrétní situace **právo** kdykoli **vznést námitku proti zpracování osobních údajů**, které se jej týkají. **Správce osobní údaje dále nezpracovává**, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

Pokud se osobní údaje zpracovávají pro **účely přímého marketingu**, má subjekt údajů právo vznést kdykoli námitku proti zpracování osobních údajů, které se ho týkají, pro tento marketing, což zahrnuje i profilování, pokud se týká tohoto přímého marketingu. Pokud subjekt údajů vznesl námitku proti zpracování pro účely přímého marketingu, **nebudou již osobní údaje pro tyto účely zpracovávány** (opt-out princip). Správce požadavek subjektu údajů u subjektu poznačí, čímž **zabrání dalšímu zpracování pro tyto účely** (povede tzv. seznam Robinsonů, tzn. lidí, kteří nemají v žádném případě zájem na tom, aby jim byly jakékoliv propagační materiály zasílány). Na možnost vznést námitku by měl být subjekt osobních údajů výslovně upozorněn.

Právo nebýt předmětem automatizovaného individuálního rozhodování (čl. 22)

Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká. Neuplatní se, pokud je rozhodnutí:

- nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů;
- povoleno právem Unie nebo členského státu, které se na správce vztahuje a které rovněž stanoví vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů; nebo
- založeno na výslovném souhlasu subjektu údajů.

Omezení práv a zásad zpracování (čl. 23)

Omezení práv a zásad zpracování je možné jen v některých případech uvedených v čl. 23 Obecného nařízení.

5. Povinnosti správců osobních údajů

Hlavním subjektem, bez kterého se žádné zpracování osobních údajů neobejde, je správce osobních údajů. Správce nejen určuje účel a prostředky zpracování osobních údajů, musí také, a to je podstatné, zajistit při zpracování osobních údajů soulad s Obecným nařízením.

Na správce jsou při ochraně osobních údajů kladeny povinnosti, které vyplývají ze základních principů Obecného nařízení - z **odpovědnosti správce osobních údajů** a z **přístupu založeného na riziku**. Jedná se především o vedení záznamů o činnostech zpracování osobních údajů, posuzování vlivu zpracování osobních údajů, dále jde o konzultace s dozorovým úřadem, o ohlašování porušení zabezpečení osobních údajů a o jmenování pověřence na ochranu osobních údajů. Uvedené povinnosti se nebudou týkat všech správců, vždy bude záviset na tom, jaké zpracování osobních údajů správce provádí.

5.1 Pověřenec pro ochranu osobních údajů (oddíl 4)

Jmenovat pověřence pro ochranu osobních údajů je nová povinnost vyplývající z čl. 38 a 39 Obecného nařízení. **Tuto povinnost však mají pouze organizace, které provádějí rizikové zpracování osobních údajů.**

Pověřenec pro ochranu osobních údajů je osoba zodpovědná za zpracování osobních údajů v organizaci, jeho hlavním úkolem je být nápomocný správcům při dosahování souladu se zpracováním osobních údajů a tím chránit práva subjektů údajů u rizikových zpracování.

Povinnost jmenovat pověřence má organizace pokud:

- zpracování provádí **orgán veřejné moci** či **veřejný subjekt**,
- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují **rozsáhlé pravidelné a systematické monitorování subjektů údajů**,
- hlavní činnosti správce nebo zpracovatele spočívají **v rozsáhlém zpracování zvláštních kategorií údajů** a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Kvalifikace pověřence:

Pověřenec musí být jmenován na základě profesních kvalit, zejména na základě odborných znalostí práva a praxe v oblasti ochrany osobních údajů (kvalifikace však nemusí být nutně právní!). Pověřenec nemusí mít certifikaci, může to být externí pracovník, jeden pověřenec může pracovat pro více organizací.

Pověřence mohou jmenovat i organizace, které nemají tuto povinnost. **Každá organizace by měla mít někoho, kdo se bude orientovat ve zpracování osobních údajů** (ale nemusí to být pověřenec dle Obecného nařízení).

5.2 Povinnost vést záznamy o činnostech zpracování (čl. 30)

Tuto povinnost mají organizace s více než 250 zaměstnanci a dále organizace provádějící zpracování, které představuje riziko pro práva a svobody fyzické osoby, přičemž nejde jen o příležitostné zpracování, nebo organizace, které zpracovávají zvláštní kategorie osobních údajů.

Povinnost vést záznamy o činnostech zpracování spadá na správce i na zpracovatele, který provádí zpracování pro správce.

Záznamy o zpracování mají obsahovat především tyto údaje:

- jméno a kontaktní údaje správce, případně pověřence pro ochranu osobních údajů;
- účely zpracování;
- popis kategorií subjektů údajů a kategorií osobních údajů;
- kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny;
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace;
- plánované lhůty pro výmaz jednotlivých kategorií údajů, je-li to možné;
- obecný popis technických a organizačních bezpečnostních opatření, je-li to možné.

Záznamy mohou mít různou podobu od jednoduchých až po sofistikované. Účelem je napomoci zorientovat se v prováděných zpracováních. Vést záznamy o činnostech zpracování lze doporučit i správcům, kteří dle Obecného nařízení tuto povinnost nemají.

5.3 Ohlašování případů porušení zabezpečení osobních údajů (čl. 33)

Porušením zabezpečení osobních údajů se podle Obecného nařízení rozumí porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

Porušení zabezpečení osobních údajů nebude nutné hlásit pokaždé. Vždy bude potřeba v první řadě vyhodnotit **závažnost porušení zabezpečení** a až na základě toho incident hlásit.

- Pokud je nepravděpodobné, že by porušení mělo za následek riziko pro práva a svobody fyzických osob, není nutné incident hlásit.

- Pokud dojde při zpracování osobních údajů k porušení jejich zabezpečení, které představuje riziko pro práva a svobody fyzických osob, je správce povinen toto nahlásit bez zbytečného odkladu, pokud možno do 72 hodin, příslušnému dozorovému úřadu.
- V určitých případech, pokud existuje pravděpodobnost vysokého rizika pro práva a svobody jednotlivců, musí správce, kromě ohlášení dozorovému úřadu, případ porušení oznámit také dotčeným jednotlivcům (subjektům osobních údajů).

Ohlašování případů porušení zabezpečení osobních údajů se vztahuje i na zpracovatele. Pokud dojde k porušení zabezpečení osobních údajů u zpracovatele, je povinen toto bez zbytečného odkladu nahlásit správci.

Ohlášení porušení zabezpečení osobních údajů musí obsahovat:

- Popis porušení zabezpečení osobních údajů, kategorie a přibližný počet dotčených subjektů údajů, kategorie a přibližný počet dotčených záznamů osobních údajů
- Kontaktní údaje správce osobních údajů, pokud správce má pověřence tak jeho kontaktní údaje.
- 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.

Správce osobních údajů má, v případě že dojde k porušení zabezpečení osobních údajů, povinnost **dokumentovat veškeré případy porušení zabezpečení osobních údajů**, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření.

6. Vztah správce a zpracovatele osobních údajů

6.1 Správce a zpracovatel osobních údajů

Správce může být jakýkoli subjekt, nerozhoduje jaké právní formy, který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně zodpovídá. Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti (např. zákonem stanovené povinnosti, ze smluv), ale může je zpracovávat i pro vlastní určené účely, např. pro své oprávněné zájmy, pokud tyto zájmy nepřevyšují zájem na ochraně základních práv a svobod fyzických osob.

Zpracovatelem je subjekt, kterého si správce najímá, aby pro něj prováděl s osobními údaji zpracovatelské operace. Jinými slovy zpracovatel zpracovává osobní údaje pro správce. Od správce se zpracovatel liší tím, že v rámci činnosti pro správce může provádět jen takové zpracovatelské operace, kterými jej správce pověří nebo které vyplývají z činnosti, pro kterou byl zpracovatel správcem pověřen. Je nutné poznamenat, že zpracovatel je zpracovatelem pouze ve vztahu k osobním údajům poskytnutým správcem, nikoli osobních údajů, které zpracovává pro účely, které se jej přímo dotýkají (např. je správcem při zpracování osobních údajů vlastních zaměstnanců). Stejně jako u správce, ani u zpracovatele není určující jeho právní forma.

6.2 Vztah správce a zpracovatele (čl. 28)

Správce si může zpracovatele přizvat ke zpracování prakticky kdykoliv, nepotřebuje k tomu souhlas subjektu údajů či jiný právní důvod pro zpracování osobních údajů. Je tomu tak z toho důvodu, že zpracovatel je vázán pokyny správce a zpracování provádí pouze pro účely definované správcem, nikoliv pro své účely.

Správce by měl využívat pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Obecného nařízení a aby byla zajištěna ochrana práv subjektu údajů.

Správce určuje zpracovateli účely a prostředky zpracování osobních údajů, čímž se od zpracovatele liší. Účel zpracování musí být legitimní a nesmí být protiprávní. Odpovědnost za zpracování osobních údajů však vždy zůstává na správci.

Smlouva

Zpracování osobních údajů zpracovatelem se řídí **smlouvou** (nebo jiným právním aktem), která **zavazuje zpracovatele vůči správci** a v které **je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce**. Tato smlouva zejména stanoví, že zpracovatel:

- zpracovává osobní údaje pouze na základě doložených pokynů správce;
- zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
- přijme bezpečnostní opatření požadovaná podle článku 32;
- dodržuje podmínky pro řetězení zpracovatelů;
- zohledňuje povahu zpracování, je správcem nápomocen při výkonu správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů;
- v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;
- poskytne správci možnost auditu, včetně inspekci prováděných správcem nebo jím pověřeným auditorem.

Smlouva musí být vyhotovena v písemné podobě (lze i elektronicky). Smlouva nemusí být samostatnou smlouvou, postačí, pokud budou požadované náležitosti upraveny v rámci jiné smlouvy.

6.3 Řetězení zpracovatelů

Řetězení zpracovatelů znamená zapojení dalšího zpracovatele do zpracování, a sice ze strany zpracovatele. Vznikne tak např. řetězec *správce* → *zpracovatel 1* → *zpracovatel 2*. Řetězení zpracovatelů může být ale různé.

Zapojení dalšího zpracovatele bez vědomí správce, tedy bez předchozího konkrétního nebo obecného písemného povolení správce, je **zakázáno**.

Pokud zpracovatel zapojí dalšího zpracovatele, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy stejné povinnosti na ochranu osobních údajů, jaké jsou uvedeny ve smlouvě mezi správcem a zpracovatelem. Neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně prvotní zpracovatel.

7. Prosazování Obecného nařízení a sankce za jeho nedodržování

7.1 Dozorový úřad (čl.51)

Každý členský stát Evropské unie má dle Obecného nařízení povinnost stanovit dozorový úřad, který bude monitorovat uplatňování Obecného nařízení. V České republice by měl být dozorový úřad stanoven zákonem o zpracování osobních údajů a bude jím pravděpodobně Úřad pro ochranu osobních údajů.

Funkce dozorového úřadu bude především poradenská a kontrolní. Dozorový úřad bude plnit důležitou roli při řešení stížností subjektů osobních údajů - na dozorový úřad se budou obracet subjekty osobních údajů, pokud budou mít podezření, že dochází ke zpracování, které je v rozporu s Obecným nařízením. Bude řešit také případy porušení zabezpečení zpracování osobních údajů - dozorovému úřadu budou správci osobních údajů hlásit případy porušení zabezpečení zpracování osobních údajů.

Předpokládá se také spolupráce mezi dozorovými úřady jednotlivých členských států EU.

7.2 Sankce a ukládání pokut (čl. 83, 84)

Porušení Obecného nařízení lze rozdělit podle závažnosti do dvou kategorií. V závislosti na závažnosti porušení Obecného nařízení je do dvou kategorií rozdělena i výše pokut, a to na:

1. pokuty do výše 10 000 000 EUR, resp. 2 % celkového ročního obratu celosvětově,
2. pokuty do výše 20 000 000 EUR, resp. 4 % celkového ročního obratu celosvětově.

Správné pokuty se ukládají podle okolností každého případu, pokuty mají být ukládány spravedlivě, je možné pokutu vůbec neuložit a místo pokuty uložit pouze některé z nápravných opatření (případně společně s nižší pokutou). Účelem Obecného nařízení není likvidace organizací, sankce mají mít především preventivní, odstrašující a donucující účinek.

Při rozhodování, zda uložit pokutu a v jaké výši, či zda uložit pouze některé z nápravných opatření, se budou zohledňovat různé okolnosti, např.:

- povaha, závažnost, délka trvání porušení, rozsah a účel zpracování, počet dotčených subjektů;
- kategorie dotčených osobních údajů;
- úmysl či nedbalost;
- kroky podniknuté správcem ke zmírnění škod;
- míra spolupráce s dozorovým úřadem;
- způsob oznámení incidentu dozorovému úřadu;
- atd.

8. Závěr

Informace v tomto dokumentu jsou pouze stručným shrnutím základních zásad Obecného nařízení a mají přispět k lepšímu pochopení základních pravidel pro ochranu osobních údajů platných v rámci Evropské unie. Dokument nemůže být chápán jako jediná možná interpretace Obecného nařízení ani jako návod na jeho implementaci, protože každá organizace, každý správce a každý zpracovatel osobních údajů má nastavená vnitřní pravidla a procesy pro zpracování osobních údajů rozdílně. Každá organizace, každý správce a každý zpracovatel také zpracovává osobní údaje v rozdílné míře. Konečný způsob implementace zásad Obecného nařízení tak bude vždy záviset na dané organizaci.