

Ochrana osobních údajů při zajišťování BOZP a PO podle GDPR



Tomáš Neugebauer
manažer BOZP a OZO v PO

Červen 2018

Ochrana osobních údajů

Od pátku 25. května 2018 je účinné Nařízení Evropského parlamentu a Rady 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, zkráceně nazývané GDPR.

Nařízení je přímo použitelný předpis EU, a proto není transformován do žádného národního předpisu. Vydán má být tzv. adaptační zákon (o zpracování osobních údajů), který má upravit náležitosti, jež GDPR umožňuje řešit na národní úrovni (postavení ÚOOÚ atd.) a bude provádět novou trestněprávní směrnici EU.



Ochrana osobních údajů

Zatím je zároveň platný i zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

GDPR na něj navazuje. I když přináší některé novinky, podstata však zůstává zachována.

V případech, kde jsou oba předpisy ve vzájemném rozporu, se postupuje podle GDPR.

Ochranu osobních údajů řeší i občanský zákoník (§ 81 a následující), např. ve vztahu k mrtvým.



Co je a co není GDPR?

GDPR se vztahuje na zcela nebo částečně automatizované a neautomatizované zpracování osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny. Přičemž evidencí je míněn jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.

Za osobní údaj jsou považovány veškeré informace o identifikované nebo identifikovatelné fyzické osobě, tedy o fyzické osobě, kterou lze přímo nebo nepřímo identifikovat (subjekt údajů).



Co je a co není osobní údaj?

Za určitých podmínek mohou být osobním údajem i informace, které tak na první pohled nevypadají (jakýkoliv údaj o zaměstnanci je údajem osobním).

- e-mailová adresa u zaměstnavatele
- velikost bot nebo oblečení
- počet odpracovaných hodin v zaměstnání, např. při výkonu rizikové práce

Je-li člověk identifikován, všechny údaje o něm jsou údaji osobními.



Základní pojmy

Správce – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně jinými určuje účely a prostředky zpracování osobních údajů

Zpracovatel – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce

Souhlas – jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, který subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů



Základní pojmy

Zpracování osobních údajů – jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů (shromažďování, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení, pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz či zničení)



Základní pojmy

Zpracování osobních údajů – jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů (shromažďování, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení, pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz či zničení)



Základní pojmy

Anonymní údaj – údaj o fyzické osobě, který není osobním údajem (není vztažen k subjektu údajů)

Anonymizací je nevratné odstranění vazby subjektem údajů a informací.

Pseudonymizace – zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou uchovány odděleně a vztahují se na ně technická a organizační opatření k zabránění přiřazení k subjektu údajů.



Základní pojmy

Porušení zabezpečení osobních údajů – porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů



Co konkrétně GDPR požaduje?

„Toto je, ale opravdu, ale opravdu špatně položená otázka“.



Václav Klaus

GDPR stanovuje jen minimálně požadavků, zákazů apod. Stanovuje pouze obecné parametry pro zajištění ochrany osobních údajů. Nezajišťuje se plnění požadavků GDPR, ale soulad s GDPR.



Co je a co není GDPR?

Jednou ze základních novinek v GDPR je přístup na základě hodnocení předpokládaných rizik a nový princip odpovědnosti správce.

Způsob ochrany osobních údajů je přirovnáván k nové BOZP (vybudován na stejných principech).

GDPR neobsahuje specifická pravidla pro nakládání s osobními údaji a postup implementace je proto složitější. Každý správce si musí vytvořit svá pravidla, která poté musí dodržovat a zajišťovat tak soulad s GDPR (obdobně jako při zajištění BOZP). Soulad musí být schopen kontinuálně prokázat.



Co je a co není GDPR?

GDPR pojímá ochranu osobních údajů jako abstraktní oblast. Nepožaduje, aby byly splněny požadavky jím stanovené, ale aby byl vytvořen soulad s ním na základě dodržování jím stanovených zásad zajištění ochrany osobních údajů.



Zásady zpracování osobních údajů

Základními stavebními kameny pro vytvoření souladu s nařízením jsou zásady určující podmínky, za kterých smí být osobní údaje zpracovávány. Jedná se o:

- zákonnost,
- korektnost a transparentnost,
- omezení účelu,
- minimalizace údajů,
- přesnost,
- omezení uložení,
- integrita a důvěrnost,
- odpovědnost.



Zásada zákonnosti



Po lidsku,
ne podle práva.

Zpracování nesmí být v rozporu se zákonem a pouze v odpovídajícím rozsahu při splnění některé z v DGPR uvedených podmínek – pro splnění právní povinnosti, pro splnění smlouvy nebo pro opatření před přijetím smlouvy, pro ochranu životně důležitých zájmů, pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, pro účely oprávněných zájmů správce nebo třetí strany, kromě případů, kdy má přednost zájem subjektu údajů a udělení souhlasu subjektem údajů.



Zásady zpracování osobních údajů

Korektnost a transparentnost

Zajišťovat co největší míru informovanosti subjektů údajů. Nezastírat účel zpracování (ten musí být vždy předem znám a být legitimní [nestačí souhlas]).

Účelové omezení

Osobní údaje nesmí být zpracovávány k jinému účelu, než k jakému byly shromážděny. Může se jednat pouze o výslovně vyjádřené a legitimní účely (výjimka – pro účely archivace ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu a pro statistické účely).



Zásady zpracování osobních údajů

Minimalizace údajů

Zpracovávat pouze údaje, které jsou pro k dosažení účelu nezbytné, a to pouze v nutném rozsahu. Platí, čím méně údajů při zpracování, tím menší riziko pro subjekt údajů při jejich úniku.

Přesnost

Údaje musí být přesné a podle potřeby aktualizované. To však neznamená, že by správce měl povinnost vyhledávat nepřesné údaje a opravovat je.



Zásady zpracování osobních údajů

Omezení uložení

Osobní údaje mají být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Nepotřebné údaje musí být vymazány nebo anonymizovány (výjimka archivace, výzkum a statistika).

Integrita a důvěrnost

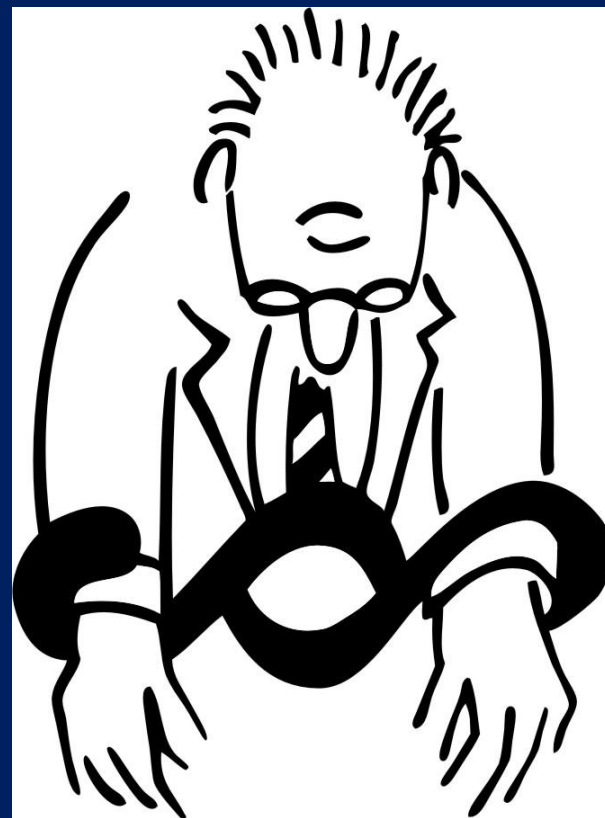
Je nutné přijmout vhodná technická a organizační opatření před neoprávněným nebo protiprávním zpracováním, jakož i před náhodnou ztrátou, zničením, poškozením.



Zásady zpracování osobních údajů

Odpovědnost

Správce odpovídá za zajištění souladu se všemi zásadami (za dodržení všech svých povinností) a musí být schopen toto prokázat (posouzení oprávněného zájmu, souhlasy, splnění informační povinnosti, vnitřní předpisy apod.).



Právní důvody zpracování

Právní důvody, které úzce souvisí s účelem zpracování (účel ovlivňuje možný právní důvod), poskytují právní základ pro zpracování osobních údajů. Souběžně může být i více právních důvodů pro zpracování osobních údajů (důležité je mít všechny zmapovány pro případ jejich postupného zanikání).



Právní důvody zpracování

Právní důvody definované v GDPR lze rozdělit do dvou základních skupin:

- bez souhlasu subjektu údajů (souhlas se nepožaduje!),
- se souhlasem subjektu údajů (souhlas je nutný).



Právní důvody zpracování

Právní důvody zpracování:

- poskytují právní základ pro zpracování osobních údajů,
- správce musí mít ke zpracování některých z důvodů,
- souvisí s účelem zpracování (účel ovlivňuje možný právní důvod zpracování),
- jsou si rovny,
- po odpadnutí posledního právního důvodu, zpravidla následuje likvidace osobních údajů.



Právní důvody nevyžadující souhlas

- zpracování je nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů nebo pro přijetí opatření před uzavřením smlouvy na žádost subjektu údajů
- zpracování je nezbytné pro plnění právní povinnosti (zásada minimalizace osobních údajů)
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby



Právní důvody nevyžadující souhlas

- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci
- zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy subjektu údajů vyžadující ochranu osobních údajů, zejména dítěte (provést tzv. test proporcionality, tj. poměření zájmu správce a zájmu subjektu údajů [práva, svobody]; podmínkou je nezbytnost) – jedná se např. o kamerový systém, přímý marketing (nabídky nové verze apod.)



Právní důvody

Všechny právní důvody jsou si rovny. Neplatí, že udělení souhlasu je nadřazeno ostatním. Naopak vyžádání si souhlasu by mělo být až poslední možnou podmínkou splnění zákonnosti, tedy až v případě, že nelze zvolit žádnou z předcházejících.

Souhlas nemá být vyžadován v případech, kdy je osobní údaj zpracováván na základě jiného právního důvodu, neboť by se tak jednalo o uvedení subjektu údajů v omyl, že zpracování údajů je odvolatelné. Také se tím zbytečně zvyšuje administrativní zátěž.



Souhlas ke zpracování

Souhlas subjektu údajů musí být dobrovolný, doložitelný, odlišitelný od ostatních údajů a odvolatelný.

Musí se jednat o svobodný, konkrétní (k jakému účelu, jaký údaj, na jakou dobu), informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením nebo jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.

Nesmí mít podobu generálního prohlášení.



Souhlas ke zpracování

Udělení souhlasu nesmí být vázáno na plnění smluvní povinnosti, např. uzavření další smlouvy. Nikdy nemá být součástí pracovní smlouvy.

Odvolání musí být stejně snadné jako jeho poskytnutí.

Dosavadní souhlasy je nutné podrobit kontrole a případně si vyžádat nové, odpovídající GDPR. Pozor však na nadbytečné vyžadování souhlasu.



Nakládání nejen s fotografiemi

Nakládání s fotografiemi, které jsou nositeli osobního údaje může být problematické. Někdy souhlas není potřeba a jindy ano (např. pro zveřejnění na nástěnce, při školení, na webu). Obdobně to platí o videích.

K použití fotografií k dokumentaci a projednání porušení požadavku BOZP nebo PO souhlas není nutný.

Pro zaslání informací obsahující osobní údaje mateřské společnosti je nejen pro fotografie nutný.



Zvláštní kategorie osobních údajů

Údaje vypovídající 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 a údaje o zdravotním stavu či sexuálním životě nebo sexuální orientaci fyzické osoby.



Zpracování zvláštních kategorií

Osobní údaje zahrnuté do zvláštních kategorií osobních údajů (dříve citlivé údaje) nesmí být zpracovávány vyjma povolených případů:

- udělení výslovného souhlasu subjektu údajů (souhlas se zpracováním svých osobních údajů k vymezenému účelu),
- zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany,



Zpracování zvláštních kategorií

- zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas,
- zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt,



Zpracování zvláštních kategorií

- zjevně zveřejněné údaje subjektu údajů,
- určení, výkon nebo obhajoba právních nároků nebo pokud soudy jednají v rámci svých pravomocí,
- veřejný zájem EU nebo členského státu,
- preventivní, pracovní lékařství, posouzení pracovní schopnosti, lékařské diagnostiky, poskytování zdravotní nebo sociální péče nebo léčby,
- veřejný zájem v oblasti veřejného zdraví,
- archivace ve veřejném zájmu, vědecký či historický výzkum.



Povinnosti správce

Správce primárně odpovídá za zpracování osobních údajů. Pro jejich ochranu je povinen zavést vhodná technická a organizační opatření odpovídající danému riziku (schopnost obnovit dostupnost osobních údajů, zajištění integrity údajů, mlčenlivost zaměstnanců atd.).

Správce je též povinen vést záznamy o činnostech zpracování. To se netýká firmy do 249 zaměstnanců, pokud zpracování pravděpodobně nepředstavuje riziko pro práva a svobody fyzické osoby, zpracování je příležitostné, nebo se **nezpracovávají zvláštní kategorie osobních údajů** (např. o zdravotním stavu), případně osobní údaje týkající se rozsudků v trestních věcech.



Povinnosti správce

Záznamy o činnostech zpracování mají být obecným přehledem o tom, co se s osobními údaji děje (mají napomoci v orientaci v systému ve firmě nebo společnosti – systémový přístup obdobně jako v BOZP).

Uloženy by měly být u osoby, která má na starosti ochranu osobních údajů.



Povinnosti správce

Záznamy o činnostech zpracování mají především obsahovat:

- totožnost správce,
- účely zpracování,
- kategorie subjektů údajů a osobních údajů,
- dobu zpracování (plánované lhůty pro výmaz) – je-li to možné,
- obecný popis technických a organizačních bezpečnostních opatření – je-li to možné.



Povinnosti správce

Správce může pro zpracování osobních údajů využít zpracovatele (například pro zpracování mezd zaměstnanců nebo zajišťování BOZP a PO).

Nezbavuje se tím však své odpovědnosti. Musí být sjednána ochrana osobních údajů (jak zabezpečena komunikace, mlčenlivost atd. Správce má provádět kontroly zpracovatele.

Zpracovatel může osobní údaje zpracovávat jen za základě pokynů správce (ujednání s ním – písemná smlouva). Musí zaručit ochranu jemu poskytovaných osobních údajů (správce po něm může např. požadovat předložení směrnice).



Povinnosti správce

Bez písemného předchozího povolení správce zpracovatel nesmí řetězit zpracovatelé osobních údajů, tedy předávat osobní údaje dalšímu zpracovateli (týká se např. „zaměstnanců“ na ŽL).

Správce je povinen o zpracovateli informovat subjekt údajů (která firma provádí zpracování, za jakým účelem).



Povinnosti správce

Smlouva mezi správcem a zpracovatelem musí být uzavřena písemně a stanovit, že zpracovatel:

- zpracovává osobní údaje pouze na základě doložených pokynů správce,
- zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti,
- přijme opatření k zabezpečení osobních údajů,
- dodržuje podmínky pro zapojení dalšího zpracovatele,
- zohledňuje povahu zpracování,
- je správci nápomocen v technických a organizačních opatřeních,



Povinnosti správce

- vymaže nebo vrátí správci osobní údaje po ukončení poskytování služeb,
- poskytne správci informace potřebné k doložení toho, že byly splněny povinnosti článku 28 (především výše uvedené), včetně auditů a inspekcí provedených správcem nebo jím pověřeným auditorem.

Zpracovatel též musí vést záznamy o činnostech zpracování.



Povinnosti správce

Nastane-li případ porušení zabezpečení osobních údajů (bezpečnostní incident), které je rizikové (např. citelná krádež dat, požár mající za následek citelnou ztrátu osobních údajů), je správce povinen to ohlásit dozorovému orgánu. Ohlášení by mělo být provedeno do 72 hod.

Oznamovací povinnost platí i ve vztahu k subjektu údajů (alespoň na veřejně přístupném místě, [není-li znám kontakt]).



Zabezpečení osobních údajů

Zabezpečení osobních údajů má být provedeno správcem, jakož i zpracovatelem, s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování a k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob.



Zabezpečení osobních údajů

Je možné, nikoliv povinné, například provést pseudonymizaci. Dále je možné provádět šifrování osobních údajů. Opět se nejedná o povinnost, ale o možnost použití v případě, kdy je to vhodné (správce usoudí, že je to potřebné).

Také musí být přijata taková opatření, aby osobní údaje zpracovávala pouze fyzická osoba, která je zpracovává na pokyn správce nebo zpracovatele. Jejich počet by měl být minimalizován.



Posouzení vlivu na ochranu osobních údajů

Správce je povinen jej provést vždy, kdy hrozí vysoké riziko pro práva a svobody subjektu údajů a též v případech systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, rozsáhlé zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů, jakož i rozsáhlé systematické monitorování veřejně přístupných prostor.



Pověřenec pro ochranu osob. údajů

Zajistit si pověřence se netýká všech správců a zpracovatelů. Ustanoven musí být pouze v případě, že zpracování osobních údajů provádí orgán veřejné moci nebo veřejný subjekt, hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů a též v případě, kdy hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií osobních údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Přesto, v každé firmě by měl být někdo, kdo má ochranu OÚ na starost.



Práva subjektu údajů

Správcem nesmí být ignorována práva subjektů údajů – právo na informace, na přístup k osobním údajům, na opravu na doplnění, na přenositelnost a na jejich výmaz. Výkon těchto práv musí být bezplatný, vyjma případů zjevně nedůvodných žádostí (například neustále se opakujících). Uskutečnění má být bez zbytečného odkladu, resp. do třiceti dnů.

Subjekt údajů má právo na kopii všeho, co obsahuje jeho osobní údaje, včetně i jen poznámek.



Práva subjektu údajů

V rámci informační povinnosti je především nutné při shromažďování údajů informovat o tom, proč je potřeba je zpracovávat, kdo a jakým způsobem je bude zpracovávat a komu mohou být údaje zpřístupněny.

V rámci přístupu k údajům je nutné poskytnout potvrzení o tom, zda jsou zpracovávány osobní údaje. Pokud ano, umožnit dálkový přístup k nim (elektronická verze). Na žádost poskytnout kopie údajů.

Právo na výmaz není právem absolutním (netýká se plnění právní povinnosti).

Právo na přenositelnost se týká digitálního zpracování.



Práva subjektu údajů

Kdokoliv, kdo v důsledku porušení GDPR utrpěl hmotnou či nehmotnou újmu, má právo od správce nebo zpracovatele obdržet náhradu utrpěné újmy.



Hrozí dokonce i trestněprávní odpovědnost.



Pokuty

Pokuty, mají mít především preventivní, odstrašující a donucující účinek, nikoliv likvidační.

Stanovená pokuta do výše 20 000 000 EUR nebo do 4 % celosvětového obrátu za předchozí finanční rok (podle toho, která hodnota je vyšší) se vztahuje pouze na závažnější porušení (porušení práv subjektu údajů, předávání osobních údajů atd.). Pro ta méně závažná (nenahlášení nebo neoznámení případu porušení zabezpečení osobních údajů atd.) jsou stanoveny poloviční hodnoty.

