Informační bezpečnost

Informační bezpečnost je soubor procesů, opatření, technologií a organizačních postupů, jejichž cílem je chránit důvěrnost, integritu a dostupnost informací a informačních systémů. Cílem je tedy zabránit neoprávněnému přístupu k citlivým datům, zajistit, že data nebudou nechtěně změněna či zničena, a zajistit, aby k nim oprávnění uživatelé měli přístup vždy, když je potřebují.

Neustálý růst hodnoty dat (osobní údaje, duševní vlastnictví, finanční informace) a sofistikovanost kybernetických útoků (ransomware, phishing, APT – Advanced Persistent Threat) vede k permanentnímu rozvoji metod, technologií a standardů v informační bezpečnosti. Firmy, instituce i jednotlivci jsou motivováni chránit svá data, což je podpořeno i legislativními požadavky.

GDPR

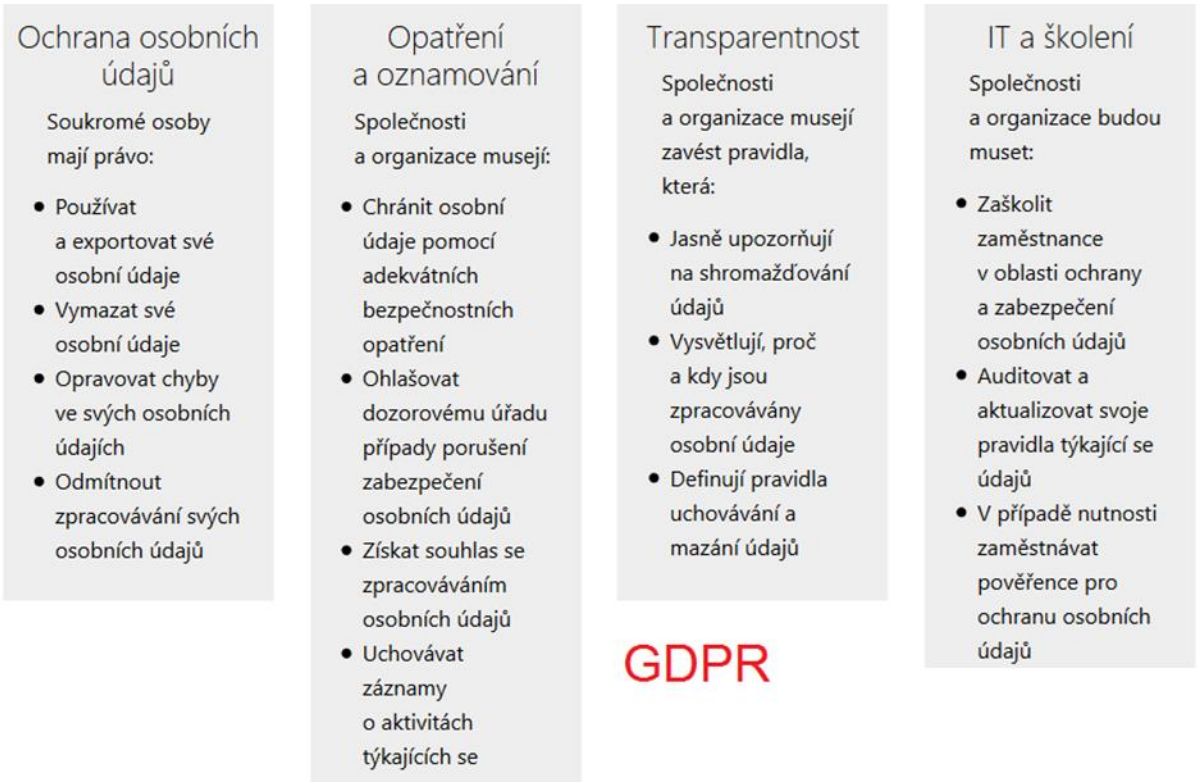
GDPR je právní předpis Evropské unie (Nařízení (EU) 2016/679), který stanoví jednotná pravidla pro ochranu osobních údajů na území EU. Cílem GDPR je posílit práva a kontrolu občanů nad jejich osobními daty a sjednotit pravidla pro organizace zpracovávající osobní údaje.

- GDPR bylo schváleno Evropským parlamentem a Radou Evropské unie v dubnu 2016 po několikaletých jednáních a přípravách.
- Nařízení nabylo účinnosti 25. května 2018.
- Předchůdcem GDPR byla Směrnice 95/46/ES, která stanovila rámec pro ochranu osobních údajů, avšak vzhledem k technologickému pokroku a rozdílům v implementaci v jednotlivých členských státech EU bylo potřeba modernizovat a sjednotit legislativu.

Hlavní cíle GDPR

- Rozšířená definice osobních údajů: Osobními údaji je prakticky jakákoliv informace, která může vést k identifikaci fyzické osoby (např. jméno, e-mail, IP adresa, GPS poloha, biometrická data).
- Transparentnost a informovaný souhlas: Organizace musí jasně a srozumitelně informovat o účelu, rozsahu a způsobu zpracování údajů a získat k tomu platný a dobrovolný souhlas subjektu údajů (pokud není zpracování opřeno o jiný právní titul, jako je např. smlouva či zákonná povinnost).
- Práva subjektů údajů: Subjekty údajů mají řadu práv, jako je právo na přístup k vlastním údajům, právo na opravu, právo na výmaz (tzv. „právo být zapomenut“), právo na přenositelnost dat a právo vznést námitku proti zpracování.
- Zásady zpracování údajů: Zpracování musí být zákonné, korektní, transparentní, účelné, minimalizované a bezpečné.
- Povinnost ohlásit únik dat: V případě porušení zabezpečení, které může představovat riziko pro subjekty údajů, je správce povinen toto nahlásit dozorovému úřadu do 72 hodin a v některých případech i subjektům údajů.
- Přísné sankce: V případě porušení GDPR hrozí vysoké finanční sankce až do výše 20 milionů eur nebo 4 % celosvětového ročního obratu, podle toho, která hodnota je vyšší.
- Zásada „privacy by design a by default“: Ochrana osobních údajů by měla být zohledňována již při návrhu systémů a procesů a měla by být výchozím nastavením (výchozí chování služeb by mělo být z pohledu ochrany soukromí co nejpřísnější).

Základní oblasti implementace GDPR



Klíčové pojmy

Osobní údaje

Osobní údaje jsou jakékoli informace týkající se identifikované nebo identifikovatelné fyzické osoby. Identifikovatelná fyzická osoba je taková, kterou lze přímo či nepřímo určit, a to zejména na základě údajů, jako je jméno, identifikační číslo (např. rodné číslo, číslo občanského průkazu), lokační údaje, online identifikátor (např. IP adresa, cookie) nebo jeden či více prvků specifických pro její fyzickou, genetickou, psychickou, ekonomickou, kulturní či sociální identitu.

Příklady osobních údajů:

- Obecné osobní údaje: jméno a příjmení, adresa bydliště, datum narození, e-mailová adresa (pokud lze podle ní určit konkrétní osobu), telefonní číslo.
- Citlivé (zvláštní) osobní údaje: údaje o zdravotním stavu, biometrické údaje (otisky prstů, sken duhovky), genetické údaje, údaje o rasovém či etnickém původu, politických názorech, náboženském přesvědčení, členství v odborech či sexuální orientaci.
- Klíčovým aspektem je identifikovatelnost: Pokud lze z dané informace samostatně nebo v kombinaci s jinými údaji dovodit konkrétní fyzickou osobu, jde o osobní údaj. Pokud tyto informace nejsou přímo spojeny s konkrétní osobou a nelze ji jimi nijak identifikovat, již se o osobní údaj nejedná.

V jakých případech se obecné nařízení o ochraně osobních údajů (GDPR) použije?

Nařízení GDPR se použije, pokud:

- podnik se sídlem v EU zpracovává osobní údaje, a to bez ohledu na to, kde skutečné zpracování údajů probíhá
- podnik je usazen mimo EU, ale zpracovává osobní údaje v souvislosti s nabídkou zboží a služeb fyzickým osobám žijícím v EU nebo sleduje chování jednotlivců v EU.

Podniky, které nejsou usazeny v EU, ale zpracovávají údaje občanů Unie, musejí jmenovat svého zástupce v EU.

Zvláštní kategorie údajů

Nesmíte zpracovávat osobní údaje o:

- rasovém či etnickém původu
- sexuální orientaci
- politických názorech
- náboženském nebo filozofickém přesvědčení
- členství v odborech
- genetických údajích, biometrických údajích či údajích o zdravotním stavu kromě specifických případů (např. pokud vám byl udělen výslovný souhlas nebo pokud je zpracování těchto údajů nezbytné z důvodu významného veřejného zájmu na základě práva EU nebo členského státu)
- osobních údajích týkajících se rozsudků v trestních věcech a trestných činů, není-li to oprávněné podle práva EU nebo členského státu.

Ve kterých případech je povoleno data zpracovávat?

Pravidla EU pro ochranu osobních údajů stanoví, že byste měli údaje zpracovávat korektním a zákonným způsobem, pro určitý a legitimní účel a měli byste zpracovávat pouze údaje nezbytné ke splnění tohoto účelu. Musíte při tom zajistit splnění některé z následujících podmínek zpracování osobních údajů. Tedy, že:

- vám dotčený jednotlivec dal se zpracováním svých údajů souhlas
- osobní údaje potřebujete z důvodu splnění smluvní povinnosti, která vás k tomuto jednotlivci váže
- osobní údaje potřebujete z důvodu splnění právní povinnosti
- osobní údaje potřebujete z důvodu ochrany životně důležitých zájmů daného jednotlivce
- osobní údaje zpracováváte za účelem provedení úkolu ve veřejném zájmu
- jednáte v oprávněném zájmu svého podniku, a to za předpokladu, že nejsou závažně dotčena základní práva a svoboda jednotlivce, jehož údaje zpracováváte. Pokud práva jednotlivce převažují nad zájmy vašeho podniku, osobní údaje zpracovávat nemůžete.

Souhlas se zpracováním údajů

Nařízení GDPR uplatňuje přísná pravidla zpracování údajů založená na souhlasu. Účelem těchto pravidel je zajistit, aby jednotlivci rozuměli tomu, s čím souhlasí. To znamená, že souhlasu musí předcházet dotaz v jasném a běžně užívaném jazyce a samotný souhlas musí být projevem svobodné,

konkrétní, informované a jednoznačné vůle. Souhlas by měl být udělen ve formě jednoznačného potvrzení, např. zaškrtnutím políčka na internetových stránkách nebo podepsáním formuláře.

Pokud vám někdo dá souhlas se zpracováním svých osobních údajů, můžete tyto údaje zpracovávat pouze pro účely, k nimž byl tento souhlas dán. Rovněž musíte danému jednotlivci umožnit, aby tento souhlas mohl odvolat.

Subjekt údajů

Subjekt údajů (Data Subject) je fyzická osoba, k níž se vztahují zpracovávané osobní údaje. Jinými slovy, subjekt údajů je člověk, jehož data organizace (správce nebo zpracovatel) zpracovává. Podle GDPR má subjekt údajů řadu práv, která mu zaručují kontrolu nad jeho osobními údaji.

Práva subjektu údajů podle GDPR:

- **Právo na informace a transparentnost:**
  Subjekt údajů má právo být informován o tom, kdo, jak a proč jeho osobní údaje zpracovává. To zahrnuje poskytnutí jasné a srozumitelné informace o účelu zpracování, době uchování, zdrojích údajů, příjemcích a o právech, která může subjekt využít.
- **Právo na přístup k osobním údajům:**
  Subjekt údajů má právo získat potvrzení, zda jsou jeho osobní údaje zpracovávány, a pokud ano, má právo získat k nim přístup, včetně kopie zpracovávaných údajů a doplňujících informací.
- **Právo na opravu (rectifikaci):**
  Pokud jsou zpracovávané údaje nepřesné nebo neúplné, má subjekt údajů právo požadovat jejich opravu či doplnění.
- **Právo na výmaz (tzv. „právo být zapomenut“):**
  Za určitých podmínek (např. pokud již údaje nejsou potřebné k původnímu účelu, pokud subjekt odvolá souhlas a neexistuje jiný právní důvod pro zpracování, nebo pokud byly údaje zpracovány protiprávně) může subjekt údajů požadovat trvalé odstranění svých údajů.
- **Právo na omezení zpracování:**
  Subjekt údajů může za určitých okolností (např. pokud napadá přesnost údajů, nebo zpracování je protiprávní a on nechce výmaz, ale jen omezení) požadovat, aby správce omezil zpracování údajů pouze na jejich uložení a nepoužíval je dále bez souhlasu či bez dalších důvodů.
- **Právo na přenositelnost údajů:**
  V případě, že je zpracování údajů založeno na souhlasu nebo na smlouvě a probíhá automatizovaně, má subjekt údajů právo získat své osobní údaje v běžně používaném a strojově čitelném formátu, aby je mohl předat jinému správci.
- **Právo vznést námitku:**
  Subjekt údajů má právo kdykoli vznést námitku proti zpracování svých údajů na základě oprávněných zájmů správce nebo při přímém marketingu. Pokud vznesené důvody převažují, musí správce s daným zpracováním přestat.
- **Právo nebýt předmětem automatizovaného rozhodování včetně profilování:**
  Subjekt údajů má právo nebýt předmětem rozhodnutí, které je založeno výhradně na automatizovaném zpracování (např. profilování) a které má pro něj právní účinky nebo se jej obdobně významně dotýká.

Zpracování údajů

Zpracování v kontextu ochrany osobních údajů (dle GDPR) zahrnuje jakoukoli operaci nebo soubor operací, které jsou prováděny s osobními údaji či soubory osobních údajů, a to s pomocí či bez pomoci automatizovaných postupů. Jde o velmi široký pojem, který pokrývá téměř každou manipulaci s osobními údaji.

Příklady činností, které se považují za zpracování:

- Shromažďování údajů (např. získávání kontaktních informací od zákazníků)
- Záznam a ukládání údajů (např. ukládání dat do databáze, archivace)
- Uspořádání, strukturování, třídění údajů
- Úprava nebo změna údajů (opravování chyb, aktualizace adres)
- Vyhledávání či nahlížení do údajů
- Použití údajů (např. při poskytování služby)
- Předání, zpřístupnění nebo zpřístupňování údajů jiným subjektům
- Srovnávání, kombinování, sdružování údajů
- Omezení zpracování (nastavení takového režimu, kdy lze s údaji jen určitým způsobem nakládat)
- Výmaz nebo zničení údajů

Zpracování tedy není jen samotné uložení nebo předání údajů. Jakákoli operace s osobními údaji, ať už fyzická (papírové dokumenty) či elektronická, se považuje za zpracování v souladu s GDPR.

Profilování

Profilování podle GDPR je jakákoli forma automatizovaného zpracování osobních údajů, která spočívá v použití těchto osobních údajů k hodnocení určitých osobních aspektů fyzické osoby. Cílem profilování je analyzovat nebo předvídat zejména aspekty týkající se pracovního výkonu, ekonomické situace, zdraví, osobních preferencí, zájmů, spolehlivosti, chování, polohy nebo pohybu subjektu údajů.

Charakteristické rysy profilování:

- Automatizované zpracování: Profilování probíhá převážně pomocí softwarových nástrojů, algoritmů a umělé inteligence.
- Hodnotící a předpovídací prvek: Profilování není jen prosté zpracování dat, ale snaha odvodit z nich určité vlastnosti, kategorie, rizikové faktory či pravděpodobné chování jednotlivce.
- Rizika: Profilování může vést k nepřiměřeným zásahům do soukromí, diskriminaci nebo nespravedlivým rozhodnutím, pokud není prováděno transparentně a za dodržení pravidel na ochranu osobních údajů.

GDPR v souvislosti s profilováním zdůrazňuje právo subjektu údajů nebýt předmětem čistě automatizovaného rozhodování, včetně profilování, pokud má takové rozhodnutí pro subjekt právní účinky nebo se ho významně dotýká. Subjekt má právo požadovat lidský zásah, vyjádřit svůj názor či rozhodnutí napadnout.

Pseudonymizace

Pseudonymizace je proces zpracování osobních údajů, při kterém jsou údaje upraveny tak, aby je nebylo možné přímo přiřadit ke konkrétní fyzické osobě bez použití dodatečných informací. Typicky to znamená nahrazení identifikátorů (např. jména, rodného čísla) jinými prvky (např. kódem, číslicemi či znakovým řetězcem), jež samy o sobě nelze spojit s konkrétní osobou.

Hlavní rysy pseudonymizace:

- **Oddělení identifikátorů:** Přímé identifikátory (jako jméno) jsou odstraněny nebo nahrazeny kódem. K propojení pseudonymizovaných dat s konkrétní osobou je nutné použít dodatečné informace (např. klíč), které jsou uchovávány odděleně a chráněny.
- **Zvýšení bezpečnosti dat:** Pseudonymizace snižuje riziko zneužití údajů v případě, že dojde k neoprávněnému přístupu k databázi. Útočník bez přístupového klíče nedokáže jednoduše zjistit totožnost osob.
- **Na rozdíl od anonymizace:** Pseudonymizace je stále formou zpracování osobních údajů, protože existuje možnost zpětné identifikace pomocí dalších informací. U anonymizace se tato možnost úplně ztrácí, tedy zcela mizí propojení s konkrétní osobou.

Pseudonymizace je doporučovaný bezpečnostní postup dle GDPR, jelikož pomáhá snižovat rizika pro práva a svobody subjektů údajů a může usnadnit dodržování dalších povinností vyplývajících z předpisů o ochraně osobních údajů.

Záznam o činnostech zpracování (Records of Processing Activities, ROPA)

je dokument (nejčastěji ve formě tabulky nebo přehledné evidence), který **popisuje, jak, proč a jaké osobní údaje organizace zpracovává**. Vyplývá z článku 30 GDPR a je jedním z klíčových prvků prokázání souladu s nařízením (tzv. princip odpovědnosti / accountability).

Podle GDPR (čl. 30) musí záznam obsahovat alespoň:

1. **Jméno a kontaktní údaje správce (případně zpracovatele)** a všech společných správců, zástupce správce a pověřence pro ochranu osobních údajů (DPO), pokud je jmenován.
2. **Účely zpracování** – proč se údaje zpracovávají (např. pro marketing, plnění smlouvy, mzdová agenda, vedení účetnictví aj.).
3. **Popis kategorií subjektů údajů a kategorií osobních údajů** – např. „zákazníci", „zaměstnanci", „kontaktní údaje", „transakční údaje" atd.
4. **Kategorie příjemců**, kterým jsou osobní údaje zpřístupněny (např. účetní firma, poskytovatel IT služeb, dopravce, banky).
5. **Informace o předávání osobních údajů do třetích zemí** (mimo EU/EHP) nebo mezinárodním organizacím – včetně záruk, pokud jsou vyžadovány (např. standardní smluvní doložky).
6. **Lhůty pro výmaz** jednotlivých kategorií údajů, pokud je to možné.
7. **Obecný popis technických a organizačních bezpečnostních opatření** (např. šifrování, pseudonymizace, řízení přístupu, zálohování).

Správce

Správce (Controller) v kontextu ochrany osobních údajů (dle GDPR) je fyzická nebo právnická osoba, veřejný orgán, agentura či jiný subjekt, který samostatně nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Jednoduše řečeno, správce je ten, kdo rozhoduje o tom, proč (za jakým účelem) a jak (jakými způsoby a prostředky) budou osobní údaje zpracovávány.

Příklady:

- Společnost, která provozuje e-shop a shromažďuje osobní údaje zákazníků k vyřízení objednávek a marketingovým účelům, je správcem.
- Škola, která shromažďuje údaje o svých žácích pro vedení studijní agendy, je správcem.
- Zaměstnavatel, který uchovává osobní údaje zaměstnanců kvůli mzdovým, daňovým a evidenčním povinnostem, je správcem.

Role správce:

- Určuje účely zpracování: proč údaje zpracovává (např. ke splnění smlouvy, zákonné povinnosti, oprávněného zájmu nebo na základě souhlasu).
- Určuje prostředky zpracování: jakým způsobem a pomocí jakých nástrojů nebo technologií se data zpracovávají.
- Odpovídá za soulad zpracování s GDPR: musí přijímat organizační a technická opatření, vést záznamy o činnostech zpracování, umožnit subjektům údajů uplatňovat jejich práva a případně spolupracovat s dozorovým úřadem.

Správce může pro provádění konkrétních operací s daty využívat zpracovatele (Processor), kterým může být jiná firma nebo subjekt, jenž provádí zpracování dat jménem správce a podle jeho pokynů. Nicméně odpovědnost za splnění právních požadavků zůstává na správci.

Zpracovatel

Zpracovatel (Processor) v kontextu GDPR je fyzická či právnická osoba, veřejný orgán, agentura nebo jiný subjekt, který zpracovává osobní údaje jménem správce a podle jeho pokynů. Na rozdíl od správce (controller), který určuje účely a prostředky zpracování, zpracovatel se řídí tím, co správce rozhodne.

Hlavní charakteristiky zpracovatele:

- Jedná na základě pokynů správce: Zpracovatel nesmí sám rozhodovat, k čemu budou osobní údaje využity. Pouze provádí zpracování podle toho, jak mu to určí správce.
- Nepřebírá zodpovědnost za účely zpracování: Účel (důvod) a prostředky (jaké technologie nebo procesy budou použity) stanovuje správce. Zpracovatel pouze provádí technické a organizační činnosti v souladu s těmito pokyny.
- Musí zajistit dostatečnou úroveň ochrany: Přestože odpovědnost za zpracování nese primárně správce, i zpracovatel je povinen chránit osobní údaje a zajistit, aby opatření přijatá k jejich zabezpečení byla dostatečná.
- Smluvní vztah se správcem: GDPR vyžaduje, aby vztah mezi správcem a zpracovatelem byl upraven písemnou smlouvou (tzv. zpracovatelská smlouva), která jasně definuje práva a povinnosti obou stran.

Příklady:

- Externí účetní firma, která pro jinou společnost (správce) zpracovává mzdovou agendu.
- IT firma spravující databázi zákazníků pro e-shop provozovaný správcem.
- Cloudový poskytovatel hostingu, který ukládá data zákazníků správce.

Zpracovatel tedy zjednodušeně řečeno pomáhá správci s praktickou stránkou zpracování osobních údajů, ale sám nemá právo rozhodovat o tom, proč a jak se tyto údaje využívají.

Příjemce osobních údajů

je fyzická či právnická osoba, veřejný orgán, agentura nebo jiný subjekt, kterému jsou osobní údaje zpřístupněny, a to ať už jde o přímé předání, poskytnutí k nahlédnutí nebo jinou formu zpřístupnění.

Charakteristika příjemce:

- **Nezávislá entita:** Příjemce je jiný subjekt, než je původní správce nebo zpracovatel.
- **Způsob předání:** Může jít o jednorázové nebo opakované předání osobních údajů.

- **Rozdíl mezi příjemcem a správcem/zpracovatelem:** Příjemce nemusí nutně vystupovat jako správce či zpracovatel. Např. může jít o orgán státní správy, kterému jsou údaje předány na základě zákona.

Např.:

- Orgány veřejné moci (policie, soudy, finanční úřad), které získají údaje na základě zákonných oprávnění.
- Obchodní partneři, společnosti poskytující doplňkové služby, kterým správce předá údaje (např. přepravní společnosti, účetní firmy, pojišťovny).
- Příjemcem ale není subjekt, který sice může mít přístup k osobním údajům, ale jedná přímo jménem správce a v jeho prospěch (takový subjekt by byl zpracovatelem). Příjemce je tedy entitou, k níž se data dostanou z iniciativy nebo souhlasu správce, ale který primárně není pouze vykonavatelem pokynů správce.

Třetí strana

v kontextu GDPR je fyzická nebo právnická osoba, veřejný orgán, agentura nebo jiný subjekt, který není:

- subjektem údajů (tj. osobou, ke které se data vztahují),
- správcem (tj. tím, kdo určuje účel a prostředky zpracování),
- zpracovatelem (tj. tím, kdo zpracovává osobní údaje jménem správce),
- ani osobou, která je přímo podřízena správci či zpracovateli a oprávněna jejich jménem provádět zpracování.

Zjednodušeně řečeno, třetí strana je jakýkoliv subjekt „mimo" základní vztah mezi subjektem údajů, správcem a zpracovatelem. Třetí stranou může být např. externí organizace, které jsou osobní údaje zpřístupněny, aniž by jednala jménem správce nebo zpracovatele, nebo jiná entita, která nemá přímou roli v rozhodování o účelu a způsobu zpracování osobních údajů.

Příklady

Předání údajů dodavatelské firmě, která je zpracovává pro správce

- Dodavatelská firma (např. externí účetní) je **příjemcem** údajů.
- Zároveň jde o **zpracovatele** (podle smlouvy a pokynů správce).
- Není to třetí strana, protože pracuje „jménem správce".

Předání údajů partnerské společnosti, která je bude sama využívat pro vlastní marketing

- Partnerská společnost je **příjemcem** (obdrží data).
- Zároveň je **samostatným správcem**, protože určuje účel zpracování (svůj marketing).
- Může být v pozici **třetí strany**, pokud s původním správcem není ve vztahu „zpracovatel–správce".

Poskytnutí údajů policii nebo jinému státnímu orgánu

- Policie je **příjemcem** (údaje jsou jí poskytnuty).
- V daném řízení často vystupuje jako **samostatný správce** (zpracovává data pro své zákonné účely).
- Z pohledu původního správce je policie **třetí stranou** (není to jeho zpracovatel, nejedná na jeho pokyn).

Interní zaměstnanec správce

- Není považován za třetí stranu, protože jedná přímo **pod autoritou** správce.
- Není ani samostatným příjemcem – provádí činnosti v rámci správce.

Pověřenec pro ochranu osobních údajů (Data Protection Officer, DPO)

je osoba, kterou správce nebo zpracovatel (organizace) jmenuje v souladu s GDPR. Jejím hlavním úkolem je dohlížet na dodržování pravidel a předpisů týkajících se ochrany osobních údajů, radit organizaci s konkrétními postupy, poskytovat školení, provádět audity a být kontaktním místem pro dozorový úřad (v ČR Úřad pro ochranu osobních údajů) i pro subjekty údajů (občany).

Kdy je firma povinna pověřence jmenovat?

Podle **čl. 37 GDPR** je povinné jmenovat DPO zejména v těchto případech:

- **Pokud je správcem nebo zpracovatelem veřejný orgán či veřejnoprávní subjekt**

  Typicky jde o orgány státní správy, samosprávy, veřejné nemocnice, veřejné školy atd. Výjimkou jsou soudy při výkonu jejich soudní pravomoci (např. v soudním řízení).

- **Pokud hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém pravidelném a systematickém monitorování subjektů údajů**

  Například velké e-shopy či technologické firmy, které neustále sledují chování uživatelů na webu nebo v mobilních aplikacích (profilování, online marketing atp.).

  „Rozsáhlé a systematické“ monitorování se vyhodnocuje případ od případu (zahrnuje i nasazení velkého počtu sledovacích nástrojů či kamerových systémů atd.).

- **Pokud hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií (citlivých) údajů nebo údajů týkajících se trestních činů a odsouzení**

  Typicky zpracování údajů o zdraví (např. velká zdravotnická zařízení), biometrických nebo genetických údajů (laboratoře, velké kliniky), údajů o politických názorech, členství v odborech, náboženství, sexualitě atd.

  Rozsáhlost se posuzuje podle počtu subjektů údajů, množství zpracovávaných dat, délky zpracování i geografického záběru.

Pokud se firma **nenachází** v jedné z uvedených tří situací, **není jmenování pověřence** povinné. Může ho ovšem ustanovit **dobrovolně**, což často zvyšuje důvěryhodnost vůči obchodním partnerům a zákazníkům a usnadňuje dodržování GDPR.

Postavení pověřence v organizaci

- **Nezávislost**: DPO nesmí být penalizován za výkon své funkce, musí být schopen působit objektivně.
- **Poradní role**: Poskytuje rady, sleduje compliance (shodu s GDPR), konzultuje posouzení vlivu na ochranu osobních údajů (DPIA).
- **Komunikační místo**: Slouží jako kontaktní osoba pro dozorový úřad a řeší dotazy subjektů údajů.
- **Odborná způsobilost**: Měl by mít znalosti z oblasti ochrany osobních údajů a IT bezpečnosti, ale GDPR striktně nedefinuje, jaké vzdělání či certifikace to musí být.

Ohlašovací povinnost

v kontextu ochrany osobních údajů (dle GDPR) znamená povinnost správce (a někdy i zpracovatele) oznámit příslušnému dozorovému úřadu a za určitých okolností i subjektům údajů, že došlo k porušení zabezpečení osobních údajů**.** Tato povinnost vychází především z **článků 33 a 34 GDPR**.

Co je „porušení zabezpečení osobních údajů" (data breach)?

GDPR definuje porušení zabezpečení (tzv. *personal data breach*) jako porušení bezpečnosti, které má za následek náhodné nebo protiprávní zničení, ztrátu, pozměnění, neoprávněné zpřístupnění nebo přístup k osobním údajům. Může jít např. o:

- Kybernetický útok (hackerský útok, ransomware),
- Neoprávněný přístup zaměstnance k údajům nad rámec jeho oprávnění,
- Ztrátu či krádež notebooku/flash disku s nešifrovanými daty,
- Odeslání dat nesprávnému příjemci (např. e-mailem).

Kdy ohlašovací povinnost vzniká?

1. Ohlášení dozorovému úřadu (v ČR je to Úřad pro ochranu osobních údajů)

V případě porušení zabezpečení, které představuje riziko pro práva a svobody fyzických osob**,** je správce povinen bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o incidentu dozvěděl, ohlásit toto porušení dozorovému úřadu.

Pokud správce nemůže oznámení učinit do 72 hodin, musí uvést důvody zpoždění a informace může dodat postupně.

Pokud správce po zhodnocení rizik dojde k závěru, že je velmi nepravděpodobné, že by z incidentu vyplynulo jakékoliv riziko (tj. bezpečnostní opatření fungovala, data byla např. šifrovaná a útočník se k obsahu nedostal), ohlášení není nutné.

2. Oznámení subjektům údajů (tj. fyzickým osobám, kterých se údaje týkají)

Pokud je porušení zabezpečení pravděpodobně spojeno s vysokým rizikem pro práva a svobody jednotlivců, musí správce informovat i dotčené fyzické osoby**.**

Výjimka: Pokud správce přijal taková opatření (např. šifrování), že data jsou nečitelná a pro útočníka bezcenná, nebo pokud by bylo informování neúměrně obtížné (pak je nutné učinit veřejné oznámení), nemusí se oznamování fyzickým osobám provádět.

Odkazy:

https://uoou.gov.cz/

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_cs.htm