Obecné nařízení č.2016/679 o ochraně osobních údajů (GDPR)

Pověřenec pro ochranu OÚ

Vedení dokumentace

Vedení dokumentace dle Nařízení

Nařízení stanovuje povinnost správce a zpracovatele (organizace) uchovávat záznamy k prokázání shody zpracování OÚ s Nařízením a v případě potřebu dozorovému orgánu soulad zdokladovat

- **dokumentace** by měla být dostatečně určitá, srozumitelná a **schopná vyjádřit soulad s Nařízením**
- **komplexnost** dokumentace by měla růst s **velikostí organizace** a dále s **rostoucí rizikovostí** zpracování
- nemusí mít pouze listinnou podobu, lze i v elektronické podobě
- měla by být **aktualizovaná v čase**

Vedení dokumentace dle Nařízení

Dokumentace vedená správcem

- identifikace jednotlivých zpracování
- dokumentace k posuzování rizik pro práva a svobody SÚ
- dokumentace k prokázání plnění jednotlivých zásad zpracování
- dokumentace k prokázání právního základu zpracování (čl.6)
- dokumentace k vyřizování žádostí k uplatnění práv SÚ
- záznamy o činnostech zpracování (čl.30)
- smlouvy o zpracování osobních údajů (čl.28)
- dokumentace k případům porušení zabezpečení OÚ (čl.33)

Vedení dokumentace dle Nařízení

Dokumentace vedená zpracovatelem

- identifikace jednotlivých zpracování
- záznamy o činnostech zpracování (čl.30)
- smlouvy o zpracování osobních údajů (čl.28)
- **písemný souhlas správce se zapojením dalšího zpracovatele**
- dokumentace k zavedení vhodných technických a organ. Opatření
- pokyny udělené podřízeným pracovníkům
- dokumentace k prokázání plnění jednotlivých zásad zpracování
- dokumentace k případům porušení zabezpečení OÚ (čl.33)

Zpracovatelská smlouva

Písemně nebo v elektronické podobě

Doporučené náležitosti zpracovatelské smlouvy :

- **předmět a doba trvání zpracování** (vymezit naprosto konkrétně)
- **povaha a účel zpracování** (např. „*vedení mzdové agendy*“)
- **typ a kategorie OÚ** (např. údaje o zdravotním stavu…)
- pokyny správce ke způsobu a formě zpracování OÚ
- **ujednání o mlčenlivosti** (zavázání pracovníků zpracovatele)
- určení konkrétních opatření k zabezpečení zpracování OÚ
- **podmínky řetězení zpracovatelů** (pouze se souhlasem správce)
- **povinnost součinnosti** zpracovatele ve vztahu ke správci a DÚ
- **povinnosti zpracovatele v případě ukončení smlouvy (výmaz OÚ)**

Práva SÚ – transparentní informace

Nařízení nově stanovuje požadavky na způsob a formu komunikace se subjekty údajů - čl.12, odst.1 Nařízení

- SÚ má být maximálně srozuměn, jakým způsobem správce nakládá s jeho OÚ
- všechny informace musí být poskytovány stručným, srozumitelným a snadno přístupným způsobem, jednoduchými jazykovými prostředky
- **informace a sdělení se poskytují písemně, e-mailem, zveřejněním na www stránkách nebo jiným vhodným způsobem**
- využívání vizualizací, „vrstvení“ informací, využívání hypertextových odkazů pro přehlednost a srozumitelnost
- nutnost úpravy dokumentace, kterou se SÚ poskytují informace

Výkon informační povinnosti

Obsah informační povinnosti (čl.13 Nařízení)

Kontaktní údaje – totožnost a kontaktní údaje správce, případně jeho zástupce a pověřence ochrany OÚ

Účel a právní základ zpracování – důvody a cíle shromažďování OÚ a právní základ pro zpracování

Oprávněné zájmy – správce je povinen SÚ o takovém zájmu informovat se současným poučením o právu vznést námitku (výslovně, zřetelně a **odděleně od ostatních informací**)

Příjemce OÚ – informace, které zpracovatele správce využívá ke zpracování OÚ, nebo kterým jiným správcům OÚ předává

Předání do zahraničí – SÚ musí obdržet informaci o tom, že správce hodlá předat jeho OÚ do země mimo EU

Práva subjektů údajů

Právo na přístup k OÚ	**Právo na opravu OÚ**
Právo na výmaz („být zapomenut“)	**Právo na přenositelnost OÚ (portabilitu)**
Právo na omezení zpracování OÚ	**Právo vznést námitku**

Výkon informační povinnosti

Vyřizování žádostí subjektů údajů

- správce musí žádost zpracovat, posoudit a odpovědět na ni bez zbytečného odkladu, nejpozději **do 1 měsíce od obdržení**

Prodloužení termínu vyřízení žádosti

- **max. o 2 měsíce**, povinnost o tom informovat žadatele s uvedením důvodů (složitost vyřízení žádosti, časové důvody..)
- po prodloužení již nebude moci správce žádost odmítnout

Odmítnutí žádosti

- pokud žádost nesplňuje předpoklady pro její vyřízení, správce o tomto musí informovat žadatele **do 1 měsíce od přijetí**
- odmítnout lze také žádost, která je nedůvodná nebo nepřiměřená

!!! Nelze v případě žádosti SÚ o poskytnutí jeho OÚ !!!

Záznamy o činnostech zpracování

Čl.30, odst.1 Nařízení

„Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá“

Čl.30, odst.2 Nařízení

„Každý zpracovatel a jeho případný zástupce vede záznamy o všech kategoriích činností zpracování prováděných pro správce…“

Povinnosti vést záznamy o činnostech zpracování nepodléhají podniky nebo organizace s méně než 250 zaměstnanci, ledaže prováděné zpracování pravděpodobně představuje riziko pro práva a svobody SÚ, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech

Záznamy o činnostech zpracování

WP29 vykládá slovo „pravidelný“ jednou nebo kombinací více následujících charakteristik:

- průběžný nebo v pravidelných intervalech a po určitou dobu se opakující
- stále se opakující nebo opakovaný ve stanovených časech
- neustále nebo pravidelně se vyskytující

WP29 vykládá slovo „systematický“ jednou nebo kombinací více následujících charakteristik:

- vyskytující se podle určitého systému
- přednastavený, organizovaný nebo metodický
- uskutečňující se jako součást obecného plánu pro sběr dat
- vykonávaný jako součást strategie

Záznamy o činnostech zpracování

Příklady činností, které mohou zakládat pravidelné a systematické monitorování subjektů údajů:

- provozování telekomunikační sítě, poskytování telekomunikačních služeb
- cílená internetová reklama
- profilování a bodování pro účely posouzení rizik
- sledování polohy (GPS, WiFi)
- **kamerové systémy**
- na těle nositelná monitorovací zařízení (zdravotní data…)
- propojená zařízení (chytré měřiče, inteligentní domy…)

Záznamy o činnostech zpracování

Záznamy správce obsahují:

- jméno - název a kontaktní údaje správce/právnické osoby
- jméno a kontaktní údaje pověřence pro ochranu OÚ (DPO)
- důvody – účely zpracování OÚ
- popis kategorií SÚ a OÚ
- kategorie příjemců, kterým byly nebo budou OÚ zpřístupněny
- informace o předání OÚ do třetí země či mezinárodní organizace

Doporučeno:

- plánované lhůty pro výmaz jednotlivých kategorií údajů
- popis technických a organizačních bezpečnostních opatření uplatňovaných při zpracování

Záznamy o činnostech zpracování

Záznamy zpracovatele obsahují:

- jméno a kontaktní údaje zpracovatele nebo zpracovatelů a všech správců, se kterými zpracovatel jedná
- jméno a kontaktní údaje pověřence pro ochranu OÚ (DPO)
- kategorie zpracování pro každého správce
- informace o předání OÚ do třetí země či mezinárodní organizace

Doporučeno:

- obecný popis technických a organizačních bezpečnostních opatření uplatňovaných při zpracování

Zabezpečení zpracování OÚ

Povinnost zabezpečení OÚ nepodléhá podle Nařízení výraznějším změnám ve vztahu ke stávající právní úpravě (Zák. č. 101/2000 Sb.)

Dle Čl.32, odst 2 Nařízení je nutné zohlednit násl. rizika:

- **„Porušení důvěrnosti“** – neoprávněné nebo náhodné **poskytnutí nebo zpřístupnění** osobních údajů
- **„Porušení dostupnosti“** – náhodná nebo neoprávněná **ztráta přístupu (trvalá, dočasná) nebo zničení** osobních údajů
- **„Porušení integrity“** – v případě neoprávněného nebo náhodného **pozměnění** osobních údajů

Nově Nařízení zavádí povinnost ohlašovat porušení zabezpečení OÚ DÚ v některých případech také SÚ, jejichž OÚ jsou ohroženy

Zabezpečení zpracování OÚ

Bezpečnostní opatření dle Nařízení (čl.32, odst.1)

Zabezpečení zpracování OÚ

Úprava přístupu fyzických osob k OÚ

Správce a zpracovatel musí přijmout taková opatření k zabezpečení OÚ a jejich zpracování, aby k nim měly přístup a zpracovávaly je pouze oprávněné osoby a jejich zpracování současně prováděly pouze podle pokynů správce

V praxi bude tento požadavek znamenat, že správce a zpracovatel bude muset své zaměstnance nebo třetí strany, které budou mít přístup k OÚ a jejich zpracování, zavázat v pracovní smlouvě (nebo dohodě o provedení práce) jednoznačnými pokyny jak s OÚ nakládat a jednoznačně zakázat nakládat s nimi v rozporu s udělenými pokyny

Směrnice

Koncepce ochrany OÚ - směrnice

Pokud je to s ohledem na rozsah zpracování přiměřené, měl by správce ve formě interního předpisu zavést interní koncepci zásad ochrany a zpracování OÚ a zveřejnit vhodná opatření, kterými by se měli řídit zaměstnanci při zpracovávání OÚ

Směrnice by měla obsahovat konkrétní pokyny pro zaměstnance, jak mají vzhledem ke specifikům dané organizace v praxi provádět zásady a povinnosti při zpracovávání OÚ v souladu s Nařízením

Porušení zabezpečení OÚ

Porušení zabezpečení, které vede k náhodnému nebo protiprávnímu (záměrnému) zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných OÚ

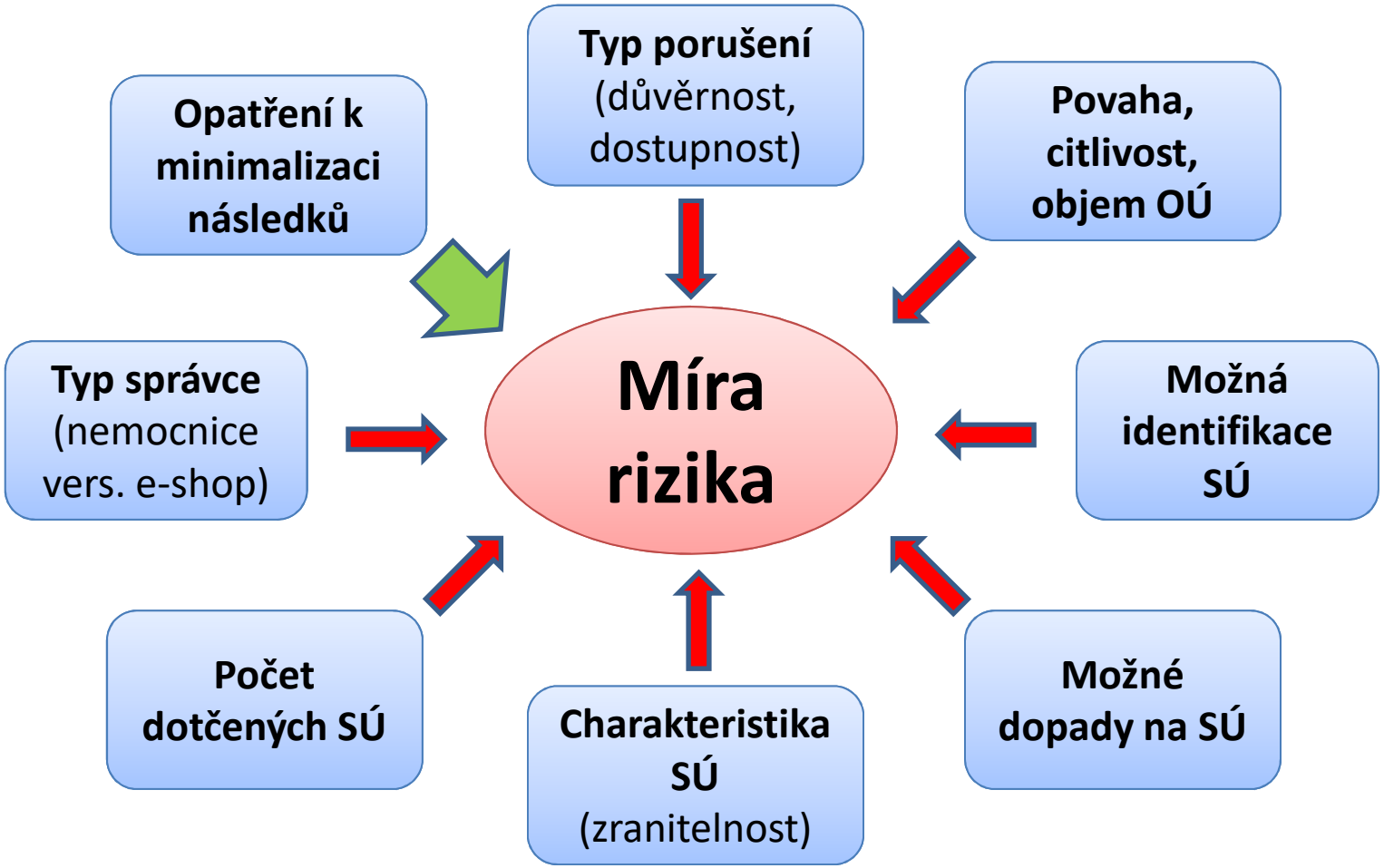
- může k němu dojít činností zvenčí (kybernetické útoky….) nebo činností zevnitř organizace (neoprávněné zpřístupnění OÚ jak úmyslně, tak z nedbalosti (!!! §180 tr. zák. – neopráv. nakl. s OÚ)

Čl.33, odst.1 Nařízení

„Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob“

Porušení zabezpečení OÚ

Možné faktory při posuzování rizika porušení



Porušení zabezpečení OÚ

Obsah ohlášení DÚ o porušení zabezpečení

Nařízení stanoví minimální obsahové náležitosti ohlášení porušení zabezpečení OÚ

a) **popis, o jaké porušení zabezpečení se v daném případě jedná**, (neoprávněný přístup nebo předání OÚ, náhodné poškození nebo zničení OÚ, …) a popsat okolnosti a průběh porušení

b) **jméno a kontaktní údaje pověřence** pro ochranu OÚ

c) **popis pravděpodobných důsledků** porušení zabezpečení OÚ

d) **popis opatření**, která SÚ přijal nebo přijme, aby vyřešil porušení nebo zmírnil jeho nepříznivé dopady především pro SÚ – **tato část je klíčová**, umožní DÚ posoudit, zda správce na porušení správně zareagoval a není tedy nutné vůči němu uplatnit pravomoci DÚ

Porušení zabezpečení OÚ

Ohlašování porušení zabezpečení zpracovatelem

Na zpracovatele se nevztahuje povinnost ohlašovat porušení zabezpečení OÚ dozorovému úřadu ani SÚ. Jakmile ovšem porušení zjistí, je povinen jej bez zbytečného odkladu oznámit správci. Nařízení přímo nestanovuje náležitosti ohlášení správci ze strany zpracovatele

Na správci leží odpovědnost za splnění ohlašovací povinnosti vůči DÚ a SÚ - zpracovatelská smlouva by měla obsahovat konkrétní ujednání o ohlašovací povinnosti zpracovatele vůči správci a o minimálním rozsahu poskytovaných informací o porušení

Porušení zabezpečení OÚ

Oznamování porušení zabezpečení subjektům údajů

Čl.34, odst.1 Nařízení

„Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů“

Př.: *e-shop umožňuje zákazníkům platby platební kartou. Údaje o platebních kartách jsou ukládány na zabezpečený server. Správce zjistí kontrolou tohoto serveru intervenci třetí osobou, která si pořídila kopie těchto údajů. Správce musí tento incident oznámit DÚ s uvedením, že může dojít k hmotné újmě dotčených SÚ. Protože se jedná o vysoké riziko pro práva a svobody fyzických osob, musí o tomto informovat i samotné SÚ*

Porušení zabezpečení OÚ

Forma a obsah oznámení porušení zabezpečení SÚ

Na formu a obsah oznámení o porušení zabezpečení subjektům údajů je třeba aplikovat formální požadavky dle čl.12 Nařízení. Mělo by být učiněno „stručným, transparentním, srozumitelným a snadno přístupným způsobem“.

Oznámení musí minimálně obsahovat:

a) **kontaktní údaje na pověřence** pro ochranu OÚ

b) **srozumitelné vysvětlení, jaké důsledky může pro SÚ porušení zabezpečení mít** (fyzická, hmotná či nehmotná újma)

c) **srozumitelný popis**, jaká **opatření** správce přijal nebo přijme s cílem **napravit porušení** zabezpečení a ke **zmírnění možných nepříznivých dopadů na SÚ**

Porušení zabezpečení OÚ

Výjimky z oznamovací povinnosti subjektům údajů

1. *v případech, kdy přijatá technická opatření zajišťují, že dotčené OÚ jsou nesrozumitelné pro kohokoli, kdo nemá oprávnění k přístupu k nim – šifrování*

2. *pokud správce po zjištění porušení zabezpečení přijme taková opatření, že se neprojeví vysoké riziko pro práva a svobody SÚ*

3. *pokud by oznámení znamenalo pro správce vynaložení nepřiměřeného úsilí – např. nemá možnost s přiměřeným úsilím získat kontaktní údaje na SÚ*