GDPR General Data Protection Regulation

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)

Hierarchie právních předpisů

Právní řád České republiky je hierarchicky uspořádán. V čele stojí Ústava a další ústavní zákony, které mají nejvyšší právní sílu a mohou být měněny zase jen ústavním zákonem. Pod ústavními zákony stojí zákony, na jejichž základě jsou vydávány prováděcí předpisy, které mají nižší právní sílu. Platí, že předpis nižší právní síly musí být vždy v souladu s předpisem vyšší právní síly. Právní předpis může být zrušen nebo změněn zásadně pouze předpisem stejné nebo vyšší právní síly.

Zvláštní postavení mají mezinárodní smlouvy. Jsou součástí právního řádu a v případě sporu mají přednost před zákonem, tj. i před ústavním zákonem ČR.

Co se týče práva evropského, platí stejně jako v ostatních členských státech EU zásada přednosti komunitárního práva. Ta stanoví, že pokud je v rozporu evropská norma s vnitrostátní normou (tj. zákonem, vyhláškou apod.) členského státu, má přednost norma evropská.

To platí pro rozpor národní normy s primárním komunitárním právem (zakládacími smlouvami) **i se sekundárním komunitárním právem** (nařízeními, směrnicemi apod.). Ze zásady přednosti nejsou dle převládajícího výkladu vyňaty ani nejvyšší zákony členských států – **evropská norma má přednost i před ústavou či ústavním zákonem členského státu.** *(čl. 10 Ústavy České republiky)*

Čl. 10: *Vyhlášené mezinárodní smlouvy, k jejichž ratifikaci dal Parlament souhlas a jimiž je Česká republika vázána, jsou součástí právního řádu; stanoví-li mezinárodní smlouva něco jiného než zákon, použije se mezinárodní smlouva.*

Zdroj: Ministerstvo spravedlnosti České republiky.

Sekundární normy EU
směrnice vs. nařízení

Směrnice

- v daném termínu členské státy provedou implementaci do vlastních právních aktů, které nesmí být v rozporu s touto směrnicí

Nařízení

- Je přímo použitelné, naopak ruší veškeré právní akty států EU, které jsou s nařízením v rozporu
- Není možná implementace do právních aktů členských států (výjimky stanoví přímo směrnice)

Základy ochrany osobních údajů

Listina základních práv a svobod

Čl. 7:

- (1) **Nedotknutelnost osoby** a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.

Čl. 10:

- (1) Každý občan má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a **chráněno jeho jméno**.
- (2) Každý má právo na **ochranu před neoprávněným zasahováním** do soukromého a rodinného života.
- (3) Každý má právo na **ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.**

Ochrana osobních údajů v našem právním řádu (1)

Soukromoprávní:

Občanský zákoník

§ 3 – ochrana života, zdraví, svobody, důstojnosti, soukromí a svobody

§ 12 – soudní ochrana soukromých práv

§ 77 – právo na ochranu osobního jména (jméno a příjmení)

§ 79 – právo přijmout pseudonym – veřejně známý pseudonym má stejnou ochranu jako jméno

§ 81 – osobnost člověka – ochrana důstojnosti, vážnosti, ctí, soukromí a projevy osobní povahy

Veřejnoprávní:

Dříve: Zákon č. 101/2000 Sb. O ochraně osobních údajů.

Od 25.5.2018 GDPR

Úprava vyvolána podmínkami informační společnosti – snadné operace s velkým množství dat, možné zneužití.

Zákon č. 110/2019 Sb., o zpracování osobních údajů

Ochrana osobních údajů v našem právním řádu (2)

Také trestním právem – zákon č. 40/2009 Sb., trestní zákoník:

§ 180

Neoprávněné nakládání s osobními údaji

(1) Kdo, byť z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.

Ochrana v mezinárodních smlouvách a právu EU

OSN – Všeobecná deklarace lidských práv *(zejm. č. 12)*

Rada Evropy

- Úmluva o ochraně lidských práv a základních svobod *(čl. 8) – ČR od 1992*
- Úmluva o ochraně osob se zřetelem na automatizované zpracování dat *(čl.8) – ČR od 2011*

EU

- Směrnice 46/95/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů – *(vycházel z ní zákon č. 101/2000 Sb. O ochraně osobních údajů) – zrušena přijetím GDPR*
- Listina základních práv *(čl. 8)*

Listina základních práv EU

Článek 8

Ochrana údajů

1. Každý má právo na ochranu osobních údajů, které se ho týkají.
2. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.
3. Na dodržování těchto pravidel dohlíží nezávislý orgán.

GDPR (General Data Protection Regulation)

Nařízení Evropského parlamentu a Rady EU 2016/679
o ochraně fyzických osob v souvislosti se zpracováním osobních údajů
a o volném pohybu těchto údajů

Jinak:

Obecné nařízení o ochraně osobních údajů

Účinné od 25. května 2018

Právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva jejích občanů proti neoprávněnému zacházení s jejich daty a osobními údaji.

Přímo závazný předpis, přímo použitelný ve smyslu vymahatelnosti práva. Tam, kde je možná úprava jednotlivými členskými státy, je uvedeno přímo v ustanoveních tohoto nařízení *(např. čl. 23 a 87 – 90)*

Co to je: zpracování osobních údajů..

- Jakákoli operace nebo soubor operací s osobními údaji
- S pomocí či bez pomoci automatizovaných postupů *(musí být obsaženy v evidenci nebo do ní mají být zařazeny čl. 2 odst.1 ON)*
  - *Evidence je strukturovaný soubor osobních údajů, který je přístupný podle zvláštních kritérií nebo jsou systematicky uspořádány podle určených kritérií (např. kartotéky, lékařské kartotéky s osobními údaji v listinné podobě).*
- Příklady zpracování osobních údajů
  - *Shromažďování, zaznamenávání, uspořádávání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení*

Co NENÍ zpracování osobních údajů 1 :

- Manuální zpracování fyzických kopií dokumentů obsahujících osobní údaje, které nejsou nijak rozřazeny či evidovány podle nějakého systému (klíče)
- Pořízení a použití jednotlivých fotografií či časově omezeného obrazového záznamu (schůze, kulturní akce), aniž se vytváří souběžná evidence obsahující jméno, příjmení atd., aniž jsou systematicky přiřazovány další údaje vedoucí k identifikaci osob

POZOR: na toto se vztahuje ochrana osobnosti podle občanského zákoníku a dalších předpisů

Důležité definice, pojmy 1:

- **Subjekt údajů = Identifikovatelná fyzická osoba:**

Je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, příjmení, identifikační číslo, lokalizační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

- **Osobní údaj:**

Jsou veškeré údaje a informace o identifikované nebo identifikovatelné fyzické osobě.

- **Zvláštní kategorie osobních údajů (citlivé údaje):**

Jsou údaje o rasovém či etnickém původu, politických názorech, náboženském vyznání či politickém přesvědčení, členství v odborech, genetické údaje a biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu, sexuálním životě nebo sexuální orientaci. Také údaje o trestných činech vč. trestních rozsudků a souvisejících bezpečnostních opatření – pod dozorem orgánu veřejné moci nebo oprávněné podle zákona (např. doklad o trestněprávní bezúhonnosti, výpis z rejstříku trestů).

Obecně platí, že zpracovávání těchto údajů je ZAKÁZÁNO. Výjimky pro zpracování stanoví čl. 9, odst. 2 ON.

Důležité definice, pojmy 2:

- **SPRÁVCE** - osoba, orgán veřejné moci, agentura atd., který určuje účely a prostředky zpracování osobních údajů.
  - Odpovídá za dodržování zásad zpracovávání osobních údajů, přičemž toto dodržování musí být schopen doložit
  - Institut společného správce – v případě, že účel a prostředky stanoví společně dva nebo více správců za vymezení podílů na odpovědnosti
- **ZPRACOVATEL** - je ten, kdo zpracovává osobní údaje pro správce (pro tuto činnost je pověřen správcem na základě smlouvy či přímo na základě zákonného ustanovení)
  - Odpovídá za dodržování zásad zpracovávání osobních údajů, přičemž toto dodržování musí být schopen doložit
  - *Čl. 28 odst. 3 písm. h): Zpracovatel sice není primárně zodpovědný za zákonnost (právní titul, právní základ), ALE MUSÍ SI UČINIT NA TO NÁZOR. Tzn., že pokud má za to, že je porušováno obecné nařízení o ochraně osobních údajů, je POVINEN NEPRODLENĚ INFORMOVAT SPRÁVCE.*

POZOR:

Vztah správce – zpracovatel je smluvně sjednán, není nutná samostatná smlouva, viz čl. 28 odst. 3 ON.

EDPB – Pokyny č. 07/2020 k pojmům správce a zpracovatel – nově 7. července 2021

Důležité definice, pojmy 3:

Příjemce:

JE ten, komu jsou osobní údaje zpřístupněny (včetně samotného subjektu údajů, správce, zpracovatele atd.)

NENÍ inspekční orán, vyšetřovací orgán (např. Česká obchodní inspekce, Finanční úřad, Úřad pro ochranu hospodářské soutěže, Policie atd.) – jedná se o šetření na základě zvláštního zákona – čl. 4/9 Obecného nařízení

Omezení zpracování:

Označení uložených osobních údajů tak, aby bylo možné vyřadit je ze zpracování – čl. 4/3 Obecného nařízení

Profilování:

Automatizované hodnocení či vyhodnocování osobních aspektů, jako je rozbor nebo odhad určitého výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa kde se nachází, nebo pohybu.

Pseudonymizace:

Osobní údaje nelze přiřadit konkrétní osobě (subjektu údajů) bez dodatečných informací, které zároveň musí být uchovávány odděleně a zabezpečeny před použitím neoprávněnými osobami.

Základní zásady zpracování podle

8 základních zásad zpracování osobních údajů čl. 5 ON

1. ZÁKONNOST – (údaje jsou zpracovávány na základě zákonného zmocnění), viz dále – *hlavní povinnost správce*
2. KOREKTNOST A TRANSPARENTNOST – (informace, požadavky) viz dále – *práva subjektu údajů a tím pádem povinnost*
3. ÚČELOVOST – (určité, výslovné a legitimní účely zpracování)
4. MINIMALIZACE ÚDAJŮ – (přiměřené, relevantní a omezené na nezbytný rozsah zpracovávaný osobních údajů)
5. PŘESNOST – (přesné, popř. nutně aktualizované údaje)
6. OMEZENÍ ULOŽENÍ – (uložení po dobu nezbytně nutnou pro daný účel, popř. doba určena zvláštními předpisy – archivační a skartační lhůty)
7. INTEGRITA A DŮVĚRNOST – (náležité zabezpečení, hlášení incidentů)
8. OPOVĚDNOST SPRÁVCE – (odpovědnost a povinnost doložit – pod hrozbou sankce až 20 000 000 €, např. nutné pořizovat záznamy o zpracování)

1. ZÁKONNOST

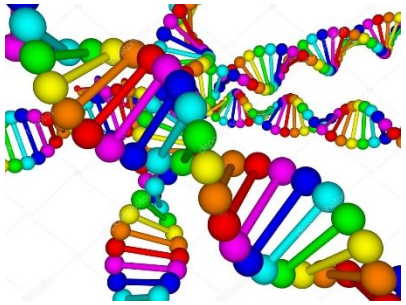
ZÁKONNOST ZPRACOVÁNÍ
čl. 6/1 ON

Zpracování je zákonné, jen pokud je splněna nejméně jedna z těchto podmínek:

a) Subjekt údajů udělil souhlas se zpracováním
b) Zpracování je nezbytné pro splnění smlouvy – *jedná se i o zpracování osobních údajů vedoucí k uzavření smlouvy na žádost dotčeného subjektu údajů*
c) Zpracování je nezbytné pro splnění právní povinnosti, kterou je správce pověřen *Pozor na vymezení práva !!!*
d) Zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby
e) Zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen
f) Zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany - *omezeno testem proporcionality, zejména u dětí !!!*

V případě odstavců e) a f) se je možné podat námitku !!

ZÁKONNOST ZPRACOVÁNÍ „citlivé údaje“ čl. 9/2 ON



Zvláštní kategorie údajů – obecně se zpracování **zakazuje.**

Pouze tyto výjimky:

a) Výslovný souhlas zjevně zveřejněný subjektem údajů

b) Nezbytné v oblasti pracovního práva, sociálního zabezpečení a sociální ochrany *(pracovní úrazy, údaje o pracovní neschopnosti)*

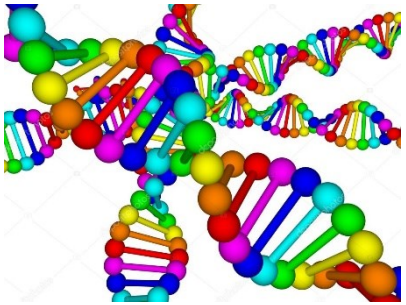
c) Zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, pokud subjekt není schopen dát souhlas

d) Nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle

e) OÚ zjevně zveřejněné subjektem údajů *(sbírka na operaci zveřejněná na Facebooku)*

f) Nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pro výkon pravomoci soudu *(návaznost na pracovně-právní spor apod., spadá do oprávněného zájmu správce, tedy právní titul pod písmenem f)*

ZÁKONNOST ZPRACOVÁNÍ „citlivé údaje“ čl. 9/2 ON



g) Zpracování je nezbytné z důvodu významného veřejného zájmu *(přidělování sociálních bytů – i zdravotní údaje žadatelů, služby sociální péče)*

h) Nezbytné pro účely preventivního nebo pracovního lékařství, posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů služeb zdravotní nebo sociální péče *(domovy pro seniory, domovy se zvláštním režimem apod.)*

i) Nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví – nutná mlčenlivost *(přeshraniční šíření nemocí – hygienická činnost)*

j) Pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely *(zákon o spisové službě)*

Souhlas čl. 4/11, čl. 7/1

Jaký musí být všeobecně:

- Svobodný - subjekt údajů má skutečnou a svobodnou volbu a může souhlas odmítnout a odvolat, aniž by byl za to „popotahován“
  - *Svobodný NENÍ, jestliže mezi subjektem údajů a správcem existuje jasná nerovnováha, zejm. v případě, kdy je správcem orgán veřejné moci*
  - *Svobodný NENÍ, jestliže je na udělení souhlasu závislé plnění smlouvy*
- Konkrétní - musí být jasné, k jakému účelu je souhlas dáván
- Informovaný – znamená mít alespoň základní informace o zpracování: kdo zpracovává a k jakému účelu.
- Odlišitelný - udělovaný souhlas není součástí jiného textu, tj. musí být zřetelně oddělen od jiných sdělení a informací
- Jednoznačný – nesmí být konstruován tak, aby dával možnost dvojího výkladu

Souhlas

Dále musí platit:

- Správce MUSÍ být po celou dobu zpracování osobních údajů schopen doložit, že má udělen souhlas se zpracováním.
  - *V případě ztráty souhlasu je nutné zpracování osobních údajů přerušit a opětovně je získat. Pokud ne, pak musíme zpracování ukončit.*
  - *Doložení je možné formou příznaku v databázi, kdy její důvěryhodnost se zajišťuje pomocí vytvoření hash otisku dokumentu.*
- Souhlas osoby mladší 13 let (týká se služeb informačních společností) – musí být potvrzen zákonným zástupcem
- Subjekt údajů musí před udělením souhlasu obdržet informace o svých právech (vzetí zpět, přístup, oprava… čl. 13 a 14)

Pozn.: souhlasy získané před účinností Obecného nařízení – pokud nejsou v souladu s Obecným nařízením, JSOU NEPLATNÉ. Je nutné provést kontrolu souhlasů, informovat subjekt údajů se změnami v dané oblasti, a ve smyslu Obecného nařízení znovu získat souhlas.

Pokyny EDPB č. 05/2020 k souhlasu podle nařízení 2016/679

Souhlas - shrnutí

Základní náležitosti	Určitost souhlasu	Forma souhlasu
• Jednoznačný • Svobodný • Konkrétní • Informovaný	• Udělen na určitou dobu • Udělen za určitým účelem	• Jasně odlišitelný • Jazykově jednoduchý • Snadno přístupný

Splnění právní povinnosti správce vs. Splnění úkolu ve veřejném zájmu (c vs. e)

- Splnění právní povinnosti správce – jedná se o zpracování osobních údajů na základě přesného zmocnění v zákoně, který provádí orgán, který je tímto zákonem stanoven
  - *Například: povinnost zaměstnavatele předávat osobní údaje zdravotní pojišťovně. Správce musí tuto povinnost specifikovanou danou normou bez výjimky splnit.*

- Splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce - není přesné zmocnění v zákoně, jedná se o volné stanovení nějakého úkolu či povinnosti v zákoně. Nejde tedy o konkrétní právní povinnost.
  - *Například: v zákonu o obcích je zakotvena povinnost obce pečovat o vytváření podmínek pro místní rozvoj sociální péče a uspokojování potřeb občanů, především o uspokojování potřeb bydlení. Z uvedeného lze tedy vyvodit oprávnění vést agendu žadatelů o přidělení sociálního bytu. Je na správci, jakou formu zvolí.*
  - *Také profesní komory a jejich činnosti.*
  - *POZOR – na nadměrné shromažďování nepotřebných údajů a aktivace možnosti podat námitku*

Oprávněný zájem správce (f)

- Oprávněný zájem správce je typicky „sporným“ užitím „právního titulu“. Klasickým případem je užití kamerového systému. Jde povětšinou o ochranu majetku správce.
- Před započetím zpracování osobních údajů je nutné posoudit
  - Skutečnou oprávněnost zpracování (tedy jestli není tento zájem postaven na „zbožném přání“ správce)
  - Jestli je zamýšlené zpracování nezbytně nutné
  - Jestli v daném případě nepřevažují zájmy či základní práva a svobody subjektu údajů nad zájmy správce. Toto se ověřuje tzv. BALANČNÍM TESTEM.

Příklad: vymáhání právních nároků

Balanční test – co je jeho součástí?

Identifikace oprávněného zájmu

- Jaký je účel zpracování?
- Je zpracování osobních údajů nutné k dosažení stanoveného cíle?

Test nutnosti

- Proč je dané zpracování důležité pro správce?
- Proč je dané zpracování důležité pro další příjemce dotčených dat, existují takoví příjemci?
- Existuje jiné řešení k dosažení cíle, bez nutnosti zpracovávat osobní data?

Balanční test

- Lze očekávat, že toto zpracování bude provedeno?
- Má zpracování osobních údajů další hodnotu k produktu či službě, kterou subjekt údajů už nyní využívá?
- Je pravděpodobné, že zpracování negativně ovlivní práva subjektu údajů?
- Je pravděpodobné, že zpracování způsobí neoprávněnou škodu či způsobí tíseň subjektu údajů?
- Atd…..

2. KOREKTNOST A TRANSPARENTNOST

Korektnost a transparentnost obecně

Typicky: zásady uplatňované při komunikaci se subjektem údajů

(co po nás tímto nařízení chce: jedná se o toky informací, změny na žádost apod. – „slohová cvičení“ sdělení jednoduchá, pochopitelná, stručná, srozumitelná)

Obecná práva subjektů údajů:

- *Právo na informace o prováděném zpracování a s tím související (čl.13,14)*
- *Právo na přístup ke svým osobním údajům (čl. 15)*
- *Právo na opravu nepřesných osobních údajů (čl. 16)*
- *Právo být zapomenut - výmaz vlastních osobních údajů (čl. 17) + příjemci*
- *Právo na omezení zpracování vlastních osobních údajů (čl.18) + příjemci*
- *Právo na přenositelnost vlastních osobních údajů (čl. 20) + příjemci*
- *Právo vznést námitku proti zpracování osobních údajů (čl. 21)*
- *Právo NEBÝT předmětem rozhodování na základě výhradně automatizovaného zpracování vlastních osobních údajů (čl. 22)*

Informace o přijatých opatřeních, bez zbytečného odkladu a v každém případě do 1 měsíce od obdržení žádosti (lze prodloužit až na 3 měsíce). Pokud odmítne přijmout opatření – informace o tom do 1 měsíce.

Korektnost a transparentnost – informace při získání OÚ čl.13-14

V okamžiku získání osobních údajů jsou subjektu údajů poskytnuty informace

- Kdo je správcem, pověřencem (je-li) a kontakty na ně
- Účel zpracování a jejich právní základ
- Kdo je příjemcem osobních údajů
- Zda se osobní údaje předávají do třetích zemí
- Dobu zpracování a následného uložení

- Právo na přístup, opravu, výmaz, omezení zpracování, podat námitku a zda je v rámci zpracovávání uplatněno automatizované rozhodování či profilování
- Právo podat stížnost u dozorového úřadu
- Informaci o právním podkladu zpracování osobních údajů, tedy zda je zákonné či smluvní a důsledky neposkytnutí
- ALE TAKÉ: zdroj osobních údajů v případě, že nejsou poskytnuty subjektem údajů (např. že pochází z veřejně dostupných zdrojů)
  - *V tomto případě v přiměřené lhůtě, nejpozději do 1 měsíce, nejpozději při první komunikaci se subjektem údajů – v případě použití těchto údajů pro účely této komunikace nebo nejpozději při prvním zpřístupnění osobních údajů jinému příjemci*

7. INTEGRITA A DŮVĚRNOST

Integrita a důvěrnost čl. 5/1/f, čl. 32 – I.

- Zabezpečení před neoprávněným zpracováním a zároveň před náhodnou ztrátou, zničením nebo poškozením
- S přihlédnutím:
  - Ke stavu techniky, nákladům
  - Povaze, rozsahu, kontextu a účelům zpracování
  - Různě pravděpodobným a různě závažným rizikům pro práva a svobody SÚ
- Příklady:
  - Pseudonymizace a šifrování
  - Zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti
  - Schopnost obnovy dostupnosti v případě incidentů
  - Pravidelné testování, posuzování a hodnocení odolnosti

Integrita a důvěrnost čl. 5/1/f, čl. 32 – II.

Bezpečnost osobních údajů – co vlastně chráníme?

1. **Technická forma nosičů** – listinné (složky, spisy), elektronické dokumenty, databáze. Data na PC, NB, sdílených discích v e-mailech atd. Zálohy – strukturovaná i nestrukturovaná data.

2. **Životní cyklus OÚ**: zdroj údajů → účel aplikace → co vše se s údaji děje → kdo k nim přistupuje (export, kopie, zpracovatel, externí administrátor) → vynášejí se technické prostředky s údaji (NB, flash – disky?) → doba uchování → zálohování → kdo jsou příjemci.

3. **Co řešíme?**
   - ✓ *Je někde v řetězci „díra“ ?*
   - ✓ *Jsou všude nastavená jasná pravidla?*
   - ✓ *Jsou tato pravidla plněna?*

Integrita a důvěrnost čl. 5/1/f, čl. 33 – III.

Incident:

- Správce – ohlásit do 72 hodin
  - Od vědomosti relevantního zaměstnance
  - Lze i postupně dle vývoje (čl. 33/4)
- Zpracovatel – ohlásit správci bez zbytečného odkladu (ihned)
- Hlášení:
  - Kategorie osobních údajů, jejich počet
  - Přibližný počet dotčených subjektů údajů
  - Přibližné množství dotčených záznamů
  - Provedená opatření

- Obvyklé nedostatky:
  - U větších informačních systémů – absence systematického hodnocení auditních záznamů
  - Nedostatečně aplikovaná a prosazovaná pravidla pro používání hesel
  - Nedostatečná dokumentace opatření na ochranu OÚ
  - Zdokumentovat zejména:
    - Přidělování a odebírání uživatelských oprávnění
    - Povinnosti uživatelů
  - Nedostatečné zálohování dat – zůstávají na pevných discích serveru nebo externím datovém nosiči uloženém a připojeném trvale k serveru
  - Nedostatečná nebo žádná pravidla pro likvidaci dat a evidenci datových médií a práce s nimi
  - Neprovádí se kontrola dodržování bezpečnostních pravidel
  - Externí správce IT odnáší zálohy mimo prostory správce – „v dobré víře“

Standardní ochrana OÚ čl. 25

- Pro určitý účel jsou zpracovávány jen takové osobní údaje, které jsou nezbytně nutné
- Standardní ochrana = minimalizace údajů + omezení uložení
- ON však k tomu ukládá povinnost přijmout konkrétní opatření
- Shrnutí:
  - Nejmenší nezbytně nutné množství OÚ
  - Zpracovávány pouze v nezbytně nutném rozsahu
  - Uchovávány pouze po dobu nezbytně nutnou
  - Dostupné nezbytně nutnému počtu osob

Záměrná ochrana OÚ čl. 25

- Záměrná ochrana (data protection by design) → při volbě prostředků (SW, HW), i při zpracování samotném od počátku zařadit opatření pro dodržení hlavních zásad zpracování. Např.
  - SW – formulář shromažďuje jen nezbytné údaje, nepotřebné automaticky likviduje
  - Anonymizace či pseudonymizace dat (např. klientské karty – identita odděleně)
- Zohlednit především při pořizování nových aplikací, služeb, produktů, prostřednictvím veřejných zakázek a jiných výběrových řízení.
- Inspirace: osm strategií záměrné ochrany *(Evropská agentura pro síťovou a informační bezpečnost)*
  - *Minimalizace – systémy a procesy nastavit tak, aby sbíraly pouze minimum údajů*
  - *Skrývání – OÚ přístupné co nejmenšímu okruhu osob (snížení rizika)*
  - *Oddělování – OÚ jsou shromažďovány a zpracovávány odděleně, ideálně v oddělených databázích*
  - *Agregace – OÚ zpracovávat s co nejvyšší úrovní zobecnění. Přebytečné detaily likvidovat*
  - *Informování – SÚ informovat o jejich OÚ, v případě on-line přímým sdělením, přístupem k dokumentaci zpracování*
  - *Kontrola ze strany SÚ – systémy vyvíjet tak, aby umožňovaly jednoduché a efektivní uplatňování práv SÚ dle čl. 15-22*
  - *Prosazování – všechna opatření v praxi efektivně prosazovat i automatizovaně*
  - *Prokazovat omezení shromažďování pro různé účely – opatření dokumentovat.*

8. ODPOVĚDNOST SPRÁVCE

Odpovědnost správce – čl. 5/2, čl. 24-25

Správce odpovídá za dodržení všech povinností:

1. Zavede vhodná technická a organizační opatření
2. Musí být schopen dodržení souladu doložit
   - Vede záznamy o činnostech zpracování
   - Uchovává důkazy ohledně všech opatření (posouzení, dokumentace systémů zpracování, popisy bezpečnostních opatření, důkazy udělených souhlasech se zpracováním, o splnění informační povinnosti)

Záměrná ochrana = vhodná technická a organizační opatření

- Při určení prostředků pro zpracování
- V době zpracování
- Na základě posouzení závažnosti rizik pro práva a svobody subjektů údajů
- Například
  - Minimalizace – systémy nastavit tak, aby sbíraly minimum údajů
  - Skrývání – OÚ přístupné dle rolí
  - Oddělování – OÚ zpracovávány a uchovávány odděleně – v různých oddělených databázích
  - Agregace – co nejvyšší úroveň zobecnění – likvidace přebytečných detailů
  - Informování subjektů údajů a kontrola z jejich strany

Standardní ochrana = vhodná organizační a bezpečnostní opatření

- K zajištění aby standardně byly zpracovávány jen osobní údaje nezbytně nutné
- Konkrétní opatření k minimalizaci a omezení uložení.

Otázky ohledně zabezpečení osobních údajů

Jak musí správce zabezpečit osobní údaje?

Přijetím adekvátních technických a organizačních opatření ve smyslu čl. 32 ON. Nepovinné prvky zabezpečení: pseudonymizace a šifrování. Jejich dobrovolné nasazení může správce zprostit určitých povinností – např. povinnost ohlásit případ porušení zabezpečení osobních údajů samotnému subjektu údajů.

Co to je – porušení zabezpečení osobních údajů?

Je takové porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí či zpřístupnění osobních údajů. Pokud toto porušení nese velké riziko pro práva a svobody fyzických osob, je nutné tento fakt ohlásit dozorovému úřadu a subjektu údajů. Oznámení pak popisuje povahu porušení, přijatá opatření a pravděpodobné důsledky, kontaktní údaje na pověřence pro ochranu osobních údajů, byl-li ustanoven.

Jak se určuje míra rizika porušení zabezpečení?

Především se vychází z kategorie osobních údajů, jichž se porušení týká., charakteru porušení a počtu dotčených subjektů. Dalším kritériem pro určení je to, zda došlo k porušení úmyslné či nedbalostní.


POMŮŽU TI NAJÍT TY HACKERY..
... DEJ MI HESLO
kreslenyvtip.cz

Děkuji za pozornost

Mgr. Eva Cupáková
eva.cupakova@uoou.cz