

GDPR

**NARIADENIE EURÓPSKEHO
PARLAMENTU A RADY (EÚ)
2016/679 z 27. apríla 2016 o
ochrane fyzických osôb pri
spracúvaní osobných údajov a
o voľnom pohybe takýchto
údajov**

**Zákon NRSR č. 18/2018 Z. z. o
ochrane osobných údajov**

GDPR

Legislatíva GDPR

Predmet úpravy

- ochranu práv fyzických osôb pred neoprávneným spracúvaním ich osobných údajov,
- práva, povinnosti a zodpovednosť pri spracúvaní osobných údajov fyzických osôb,
- postavenie, pôsobnosť a organizáciu Úradu na ochranu osobných údajov Slovenskej republiky (jediný dozorný orgán v SR)

GDPR

Legislatíva GDPR

Osobnými údajmi sú

údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

GDPR

Legislatíva GDPR

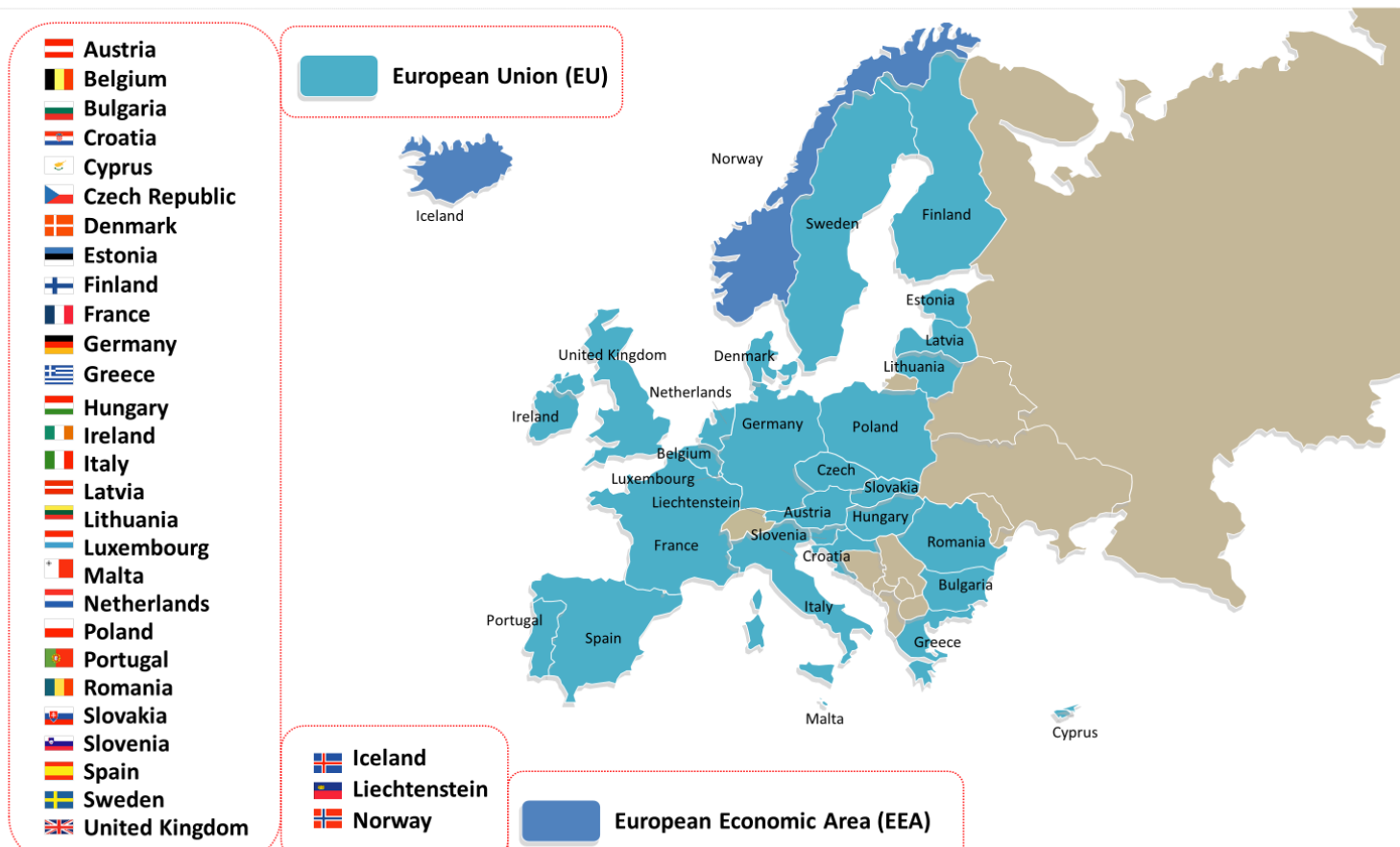
Pôsobnosť zákona

vzťahuje sa na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie osobných údajov inými než automatizovanými prostriedkami, ak ide o osobné údaje, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.

GDPR

Územná pôsobnosť

Personal Data from
28 EU and as well as 3 EEA member states



GDPR

Územná pôsobnosť

Spracovanie OÚ prevádzkovateľa alebo sprostredkovateľa USADENÉHO v SR /miesto podnikania, sídlo, org. Zložka, prevádzkareň, trvalý pobyt

Nie je usadený v SR, ale v mieste kde je usadený sa na základe medzinárodného práva verejného uplatňuje právny poriadok SR

Vzťahuje sa aj na spracovanie OÚ dotknutej osoby, ktorá sa nachádza na území SR, prevádzkovateľom alebo sprostredkovateľom, ktorý je usadený mimo SR, mimo EU, pričom spracovanie OÚ súvisí

1. s ponukou tovarov a služieb tejto dotknutej osoby na území SR, bez ohľadu či sa od dotknutej osoby vyžaduje platba alebo nie,
2. so sledovaním jej správania na území SR.

GDPR

Územná pôsobnosť

Zákon sa nevzťahuje na spracovanie osobných údajov

- Fyzickou osobou v rámci výlučne osobnej činnosti alebo domácej činnosti,
- SIS, Vojenským spravodajstvom
- NBÚ na účely vykonávania bezpečnostných previerok a na účely zabezpečovania podkladov na rozhodovanie Súdnej rady SR o splnení predpokladov sudcovskej spôsobilosti

GDPR

Legislatíva GDPR

Vymedzenie základných pojmov

-**profilovaním** akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom,

GDPR

Legislatíva GDPR

- pseudonymizáciou** spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej fyzickej osobe alebo identifikovateľnej fyzickej osobe,
- logom** záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme,
- šifrovaním** transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo,

GDPR

Vymedzenie základných pojmov

- online identifikátorom** identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä **IP adresa, cookies, prihlasovacie údaje do online služieb**, rádiovfrekvenčná identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu,
- informačným systémom** akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe,
- porušením ochrany osobných údajov** porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim,
- dotknutou osobou** každá fyzická osoba, ktorej osobné údaje sa spracúvajú,

GDPR

Vymedzenie základných pojmov

- prevádzkovateľom** každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene,
- spostredkovateľom** každý, kto spracúva osobné údaje v mene prevádzkovateľa,
- príjemcom** každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov,
- treťou stranou** každý, kto nie je dotknutou osobou, prevádzkovateľ, spostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo spostredkovateľa spracúva osobné údaje,
- zodpovednou osobou** osoba určená prevádzkovateľom alebo spostredkovateľom, ktorá plní úlohy podľa tohto zákona,

GDPR

Vymedzenie základných pojmov

-**zástupcom** fyzická osoba alebo právnická osoba so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v členskom štáte, ktorú prevádzkovateľ alebo sprostredkovateľ písomne poveril podľa § 35,

-**vnútro podnikovými pravidlami** postupy ochrany osobných údajov, ktoré dodržiava prevádzkovateľ alebo sprostredkovateľ so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území Slovenskej republiky **na účely prenosu** osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v tretej krajine,

-**kódexom správania** súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať,

GDPR

Zásady spracovania OÚ

- Zásada zákonnosti** – OÚ možno spracovať len zákonným spôsobom, aby nedošlo k porušeniu práv dotknutej osoby
- Zásada obmedzenia účelu** – len na konkrétny účel, výslovne uvedený, oprávnený
- Zásada minimalizácie osobných údajov** - spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú
- Zásada správnosti** – spracúvané OÚ musia byť správne, aktualizované. OÚ nesprávne z hľadiska účelu sa musia bez zbytočného odkladu opraviť, vymazať
- Zásada minimalizácie uchovávania** – OÚ musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú. /dlhšie na účely štatistické, archivácie, vedecké ../

GDPR

Zásady spracovania OÚ

-Zásada integrity a dôvernosti

- OÚ musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním, nezákonným spracúvaním, náhodnou stratou, výmazom alebo poškodením.

-Zásada zodpovednosti

- za dodržiavanie zásad zodpovedá prevádzkovateľ, je povinný Úradu preukázať na požiadanie dodržiavanie zásad spracovania

GDPR

Legislatíva GDPR

Zákonnosť spracúvania

Spracúvanie OU je zákonné, ak sa vykonáva na základe aspoň jedného z týchto **právnych základov**:

- Dotknutá osoba vyjadrila **súhlas**, aspoň na jeden **konkrétny účel**,
- spracúvanie je nevyhnutné na **plnenie zmluvy**, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,
- spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
- spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby,

GDPR

Legislatíva GDPR

- spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi,
- spracúvanie osobných údajov je nevyhnutné **na účel oprávnených záujmov prevádzkovateľa** alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

GDPR

Legislatíva GDPR

Podmienky poskytnutia súhlasu so spracúvaním osobných údajov

- Prevádzkovateľ je povinný kedykoľvek preukázať, že dotknutá osoba poskytla súhlas
- Ak prevádzkovateľ žiada o udelenie súhlasu na spracovanie osobných údajov dotknutú osobu, tento súhlas musí byť **odlíšený od iných skutočností** a musí byť **vyjadrený jasne a v zrozumiteľnej a ľahko dostupnej forme**.
- Dotknutá osoba má právo kedykoľvek **odvolať súhlas** so spracovaním osobných údajov, ktoré sa jej týkajú. Pred poskytnutím súhlasu musí byť o tejto skutočnosti informovaná. Môže súhlas odvolať rovnakým spôsobom, akým súhlas udelila.

GDPR

Legislatíva GDPR

Spracúvanie osobitných kategórií osobných údajov – SA ZAKAZUJE

Osobitnými kategóriami OÚ sú údaje, ktoré odhaľujú **rasový pôvod** alebo **etnický pôvod**, **politické názory**, **náboženskú vieru**, **filozofické presvedčenie**, **členstvo v odborových organizáciách**, **genetické údaje**, **biometrické údaje**, **údaje týkajúce sa zdravia** alebo údaje týkajúce sa **sexuálneho života** alebo **sexuálnej orientácie** fyzickej osoby.

GDPR

Legislatíva GDPR

Zákaz neplatí:

- pri súhlase dotknutej osoby aspoň na jeden konkrétny účel – VYSLOVNÝ SÚHLAS
- plnenia povinnosti a výkonu osobitných práv prevádzkovateľa al. DO oblasti pracovného práva, pr. soc. zabezp., verejného zdravot. Poistenia, alebo podľa kolektívnej zmluvy,
- spracúvanie je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby, ak dotknutá osoba nie je fyzicky spôsobilá alebo právne spôsobilá vyjadriť svoj súhlas,
- spracúvanie vykonáva v rámci oprávnenej činnosti **občianske združenie, nadácia** alebo nezisková organizácia poskytujúca všeobecne prospešné služby, politická strana alebo politické hnutie, **odborová organizácia**, štátom uznaná cirkev alebo náboženská spoločnosť a toto spracúvanie sa týka iba ich členov alebo tých fyzických osôb, ktoré sú s nimi vzhľadom na ich ciele v pravidelnom styku, osobné údaje slúžia výlučne pre ich vnútornú potrebu a nebudú poskytnuté príjemcovi bez písomného alebo inak hodnoverne preukázateľného súhlasu dotknutej osoby,

GDPR

Legislatíva GDPR

Spracúvanie osobitných kategórií osobných údajov – SA ZAKAZUJE

Zákaz neplatí:

- spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila,
- spracúvanie je nevyhnutné na uplatnenie právneho nároku, alebo pri výkone súdnej právomoci,
- spracúvanie je nevyhnutné z dôvodu verejného záujmu,
- spracúvanie je nevyhnutné na účel preventívneho pracovného lekárstva, poskytovania zdravotnej starostlivosti a služieb súvisiacich s poskytovaním zdravotnej starostlivosti alebo na účel vykonávania verejného zdravotného poistenia – vybrané subjekty
- spracúvanie je nevyhnutné na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel - musia byť splnené zákonné podmienky

GDPR

Legislatíva GDPR

Práva dotknutej osoby

Pri získavaní OÚ od dotknutej osoby je prevádzkovateľ povinný poskytnúť DO:

- **Identifikačné a kontaktné** údaje prevádzkovateľa,
- Kontaktné údaje **zodpovednej osoby** ak je určená,
- **Účel** spracovania OÚ, **právny základ** spracúvania,
- **oprávnené záujmy** prevádzkovateľa alebo tretej strany,
- identifikáciu príjemcu alebo kategóriu príjemcu, ak existuje,
- informáciu o tom, že prevádzkovateľ zamýšľa preniesť OÚ do tretej krajiny alebo medzinárodnej organizácii, identifikáciu tretej krajiny alebo medzinárodnej organizácie,

GDPR

Legislatíva GDPR

- doba uchovávania OÚ /kritérium jej určenia/,**
- práve požadovať od prevádzkovateľa prístup k OÚ, o práve na opravu OÚ, o práve na vymazanie OÚ alebo o práve na obmedzenie spracúvania OÚ, o práve namietat' spracúvanie OÚ, ako aj o práve na prenosnosť OÚ,**
- Práve odvolať súhlas, práve podať návrh na začatie konania o ochrane OÚ na Úrad,**
- tom, či je poskytovanie OÚ zákonnou požiadavkou alebo zmluvnou požiadavkou alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, a o tom, či je dotknutá osoba povinná poskytnúť OÚ, ako aj o možných následkoch neposkytnutia,**
- existencii automatizovaného individuálneho rozhodovania vrátane profilovania /info o postupe, o význame a dôsledkoch takéhoto spracúvavania OÚ pre DO/**

GDPR

Legislatíva GDPR

Poskytované informácie ak OÚ nie sú získané od DO:

- Kategórie** spracúvaných OÚ,
- O **zdroji**, z ktorého pochádzajú OÚ, prípadne info či pochádzajú z verejne prístupných zdrojov,

LEHOTY:

Prevádzkovateľ je povinný poskytnúť informácie:

- najneskôr **do jedného mesiaca po získaní** OÚ, pričom zohľadní konkrétne okolnosti, za ktorých sa OÚ spracúvajú,
- najneskôr v čase prvej komunikácie** s touto dotknutou osobou, ak sa OÚ majú použiť na komunikáciu s dotknutou osobou, alebo
- najneskôr vtedy, keď sa osobné údaje prvýkrát poskytnú, ak sa predpokladá poskytnutie osobných údajov ďalšiemu príjemcovi.

GDPR

Legislatíva GDPR

PRÁVO NA PRÍSTUP K OSOBNÝM ÚDAJOM

DO má právo získať od prevádzkovateľa **potvrdenie** o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, má **právo na prístup k týmto údajom a informácie o**

-účele, kategórii OÚ, dobe uchovávania

-Identifikácii príjemcu, kt. majú byť údaje poskytnuté

-Práve požadovať oprav, vymazanie, obmedzenie ich spracúvania, práve namietat spracúvanie

-Práve podať návrh na zaťažie konanie na Úrade

-ZDROJI OÚ

-Primeraných zárukách tykajúcich sa prenosu apod.

GDPR

Legislatíva GDPR

PRÁVO NA OPRAVU OÚ

DO má **právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil** nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účel spracúvania osobných údajov má dotknutá osoba **právo na doplnenie neúplných osobných údajov.**

GDPR

Legislatíva GDPR

PRÁVO NA VÝMAZ OÚ

Právo nie je absolútne /súvisí s právom na zabudnutie/

DO má **právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal OÚ**, ktoré sa jej týkajú. Ten je povinný bez zbytočného odkladu vymazať OÚ, ak DO uplatnila právo na výmaz, ak

1. OÚ už nie sú potrebné na účel, na ktorý sa získali, inak spracovali,
2. DO odvolá udelený súhlas so spracovaním, a neexistuje iný právny základ pre spracovanie, dotknutá osoba namieta spracúvanie a neprevažujú dôvody na spracúvanie,
3. OÚ sa spracúvajú nezákonne, ale. Dôvodom pre výmaz je splnenie povinností stanovených zákonom al. medzin. zmlúvou
4. sa osobné údaje získali v súvislosti s ponukou služieb informačnej spoločnosti

GDPR

Legislatíva GDPR

Ak prevádzkovateľ zverejnil osobné údaje a je povinný ich vymazať, je zároveň povinný prijať primerané bezpečnostné opatrenia vrátane technických opatrení so zreteľom na dostupnú technológiu a náklady na ich vykonanie **na účel informovania ostatných prevádzkovateľov, ktorí spracúvajú osobné údaje dotknutej osoby o jej žiadosti, aby títo prevádzkovatelia vymazali odkazy na jej osobné údaje a ich kópie alebo odpisy.**

GDPR

Legislatíva GDPR

PRÁVO NA VÝMAZ OÚ – povinnosti prevádzkovateľa sa neuplatnia, ak je spracovanie OÚ potrebné:

- na uplatnenie práva na slobodu prejavu alebo práva na informácie,
- na splnenie povinnosti podľa tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi,
- z dôvodov verejného záujmu v oblasti verejného zdravia,
- na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je pravdepodobné, že právo znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takého spracúvania, alebo
- na uplatnenie právneho nároku.

GDPR

Legislatíva GDPR

PRÁVO NA OBMEDZENIE SPRACOVANIA OÚ

DO má právo na to, aby prevádzkovateľ obmedzil spracúvanie OÚ, ak

- dotknutá osoba **namieta správnosť** osobných údajov, počas obdobia počas kt. prevádzkovateľ overuje správnosť OÚ,
- spracúvanie OÚ je **nezákonné** a dotknutá osoba namieta vymazanie OÚ a žiada namiesto toho obmedzenie ich použitia,
- prevádzkovateľ **už nepotrebuje OÚ** na účel spracúvania osobných údajov, ale potrebuje ich dotknutá osoba na uplatnenie právneho nároku, alebo
- dotknutá osoba **namieta spracúvanie OÚ**, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

Ak sa spracúvanie osobných údajov obmedzilo, okrem uchovávanía môže osobné údaje prevádzkovateľ spracúvať len so súhlasom dotknutej osoby alebo na účel uplatnenia právneho nároku, na ochranu osôb alebo z dôvodov verejného záujmu.

GDPR

Legislatíva GDPR

Právo na prenosnosť osobných údajov

Dotknutá osoba má právo získať OÚ, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v **štruktúrovanom, bežne používanom a strojovo čitateľnom formáte** a má právo preniesť tieto osobné údaje ďalšiemu prevádzkovateľovi, ak je to technicky možné a ak

- sa osobné údaje spracúvajú so súhlasom DO, dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov aspoň na jeden konkrétny účel – pri OS tzv. osobitnej kategórie, spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,
- spracúvanie osobných údajov sa vykonáva automatizovanými prostriedkami.

GDPR

Právo namietat' spracúvanie osobných údajov

1. z dôvodu týkajúceho sa jej konkrétnej situácie vykonávané podľa § 13 ods. 1 písm. e) čiže spracovanie OÚ je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo písm. f) spracovanie OÚ je nevyhnutné na účel oprávneného záujmu prevádzkovateľa alebo tretej strany, vrátane profilovania.

Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, ak nepreukáže nevyhnutné oprávnené záujmy na spracúvanie osobných údajov, ktoré prevažujú nad právami alebo záujmami dotknutej osoby, alebo dôvody na uplatnenie právneho nároku.

2. ktoré sa jej týkajú, na účel priameho marketingu vrátane profilovania v rozsahu, v akom súvisí s priamym marketingom.

Prevádzkovateľ je povinný dotknutú osobu výslovne upozorniť na práva podľa odsekov 1 a 2 najneskôr **pri prvej komunikácii s ňou**, pričom informácia o tomto práve musí byť uvedená jasne a oddelene od akýchkoľvek iných informácií.

GDPR

POVINNOSTI PREVÁDZKOVATEĽA PRI UPLATŇOVANÍ PRÁV DOTKNUTEJ OSOBY

Informačná a oznamovacia povinnosť v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne.

-Informácie poskytnúť v listinnej podobe alebo elektronickej podobe, spravidla v rovnakej podobe, v akej bola podaná žiadosť. Ak o to požiada dotknutá osoba, informácie môže prevádzkovateľ poskytnúť aj ústne, ak dotknutá osoba preukáže svoju totožnosť iným spôsobom.

-poskytnúť súčinnosť dotknutej osobe pri uplatňovaní jej práv

-Prevádzkovateľ je povinný poskytnúť dotknutej osobe informácie o opatreniach, ktoré sa prijali na základe jej žiadosti do jedného mesiaca od doručenia žiadosti /možnosť predĺžiť lehotu o ďalšie dva mesiace, a to aj opakovane/

-Ak prevádzkovateľ neprijme opatrenia na základe žiadosti dotknutej osoby, je povinný do jedného mesiaca od doručenia žiadosti informovať dotknutú osobu o dôvodoch nekonania a o možnosti podať návrh podľa § 100 na úrad.

-Bezplatne

GDPR

POVINNOSTI PREVÁDZKOVATEĽA A SPROSTREDKOVATEĽA

Prevádzkovateľ

- Na preukázanie splnenia povinností môže prevádzkovateľ použiť schválený kódex správania podľa alebo certifikát
- Prevádzkovateľ je povinný pravidelne preverovať trvanie účelu spracúvania osobných údajov a po jeho splnení bez zbytočného odkladu zabezpečiť výmaz osobných údajov; to neplatí, ak osobné údaje sú súčasťou registratúrneho záznamu.
- prijatie primeraných technických a organizačných opatrení, a na účinné zavedenie primeraných záruk ochrany osobných údajov a dodržiavanie základných zásad

GDPR

POVINNOSTI PREVÁDZKOVATEĽA A SPROSTREDKOVATEĽA

Spoloční prevádzkovatelia

- Spoločnými prevádzkovateľmi sú dvaja prevádzkovatelia alebo viacerí prevádzkovatelia, ktorí si dohodou určia účel a prostriedky spracúvania osobných údajov.
- Bez ohľadu na podmienky dohody podľa odseku 1 môže dotknutá osoba uplatniť svoje práva u každého prevádzkovateľa a voči každému prevádzkovateľovi.

GDPR

POVINNOSTI PREVÁDZKOVATEĽA A SPROSTREDKOVATEĽA

Sprostredkovateľ 1/2

- Prevádzkovateľ môže poveriť len sprostredkovateľa, ktorý poskytuje dostatočné záruky na prijatie primeraných technických a organizačných opatrení tak, aby spracúvanie osobných údajov spĺňalo požiadavky tohto zákona a aby sa zabezpečila ochrana práv dotknutej osoby
- Na poverenie sprostredkovateľa spracúvaním osobných údajov podľa prvej vety sa súhlas dotknutej osoby nevyžaduje. Údaje sa spracúvajú v mene prevádzkovateľa

GDPR

POVINNOSTI PREVÁDZKOVATEĽA A SPROSTREDKOVATEĽA

Sprostredkovateľ 2/2

- Sprostredkovateľ nesmie poveriť spracúvaním osobných údajov ďalšieho sprostredkovateľa bez predchádzajúceho osobitného písomného súhlasu prevádzkovateľa
- Spracúvanie osobných údajov sprostredkovateľom sa riadi zmluvou alebo iným právnym úkonom, ktorý zaväzuje sprostredkovateľa voči prevádzkovateľovi a v ktorom je ustanovený
 - a) predmet a doba spracúvania,
 - b) povaha a účel spracúvania,
 - c) zoznam alebo rozsah osobných údajov,
 - d) kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa.
- V zmluve alebo inom právnom úkone sa musí najmä ustanoviť, že sprostredkovateľ je povinný postupovať v zmysle §34

GDPR

POVINNOSTI PREVÁDZKOVATEĽA A SPROSTREDKOVATEĽA

Zástupca prevádzkovateľa alebo zástupca sprostredkovateľa 1/2

- Prevádzkovateľ alebo sprostredkovateľ, ktorý nemá sídlo, organizačnú zložku, prevádzkareň alebo trvalý pobyt v členskom štáte, je povinný písomne poveriť svojho zástupcu na území členského štátu, ak vykonáva spracúvanie osobných údajov dotknutej osoby, ktorá sa nachádza na území Slovenskej republiky.
- Úrad a dotknutá osoba môžu požadovať informácie týkajúce sa spracúvania osobných údajov na účely zabezpečenia súladu s týmto zákonom okrem prevádzkovateľa a sprostredkovateľa aj zástupcu prevádzkovateľa alebo zástupcu sprostredkovateľa.

GDPR

POVINNOSTI PREVÁDZKOVATEĽA A SPROSTREDKOVATEĽA

Zástupca prevádzkovateľa alebo zástupca sprostredkovateľa 2/2

- Prevádzkovateľ alebo sprostredkovateľ a zástupca prevádzkovateľa alebo zástupca sprostredkovateľa, ak bol poverený, sú povinní na požiadanie sprístupniť záznam o spracovateľských činnostiach úradu.
- Povinnosti podľa odsekov 1 a 2 sa nevzťahujú na zamestnávateľa s menej ako 250 zamestnancami, ak nie je pravdepodobné, že spracúvanie osobných údajov, ktoré vykonáva, povedie k riziku ochrany práv dotknutej osoby, ak je spracúvanie osobných údajov príležitostné alebo ak nezahŕňa osobitné kategórie osobných údajov podľa § 16 ods. 1 alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17.

GDPR

POVINNOSTI PREVÁDZKOVATEĽA A SPROSTREDKOVATEĽA

Právo na náhradu škody a zodpovednosť 1/2

- Každá osoba, ktorej vznikla majetková ujma alebo nemajetková ujma v dôsledku porušenia tohto zákona, má právo na náhradu škody²⁰⁾ od prevádzkovateľa alebo sprostredkovateľa.
- Prevádzkovateľ alebo sprostredkovateľ sa môže zbaviť zodpovednosti podľa odseku 2, ak preukáže, že vznik škody nezavinil.

GDPR

POVINNOSTI PREVÁDZKOVATEĽA A SPROSTREDKOVATEĽA

Právo na náhradu škody a zodpovednosť 2/2

- Ak sa na tom istom spracúvaní osobných údajov zúčastnil viac než jeden prevádzkovateľ alebo sprostredkovateľ alebo prevádzkovateľ aj sprostredkovateľ spoločne a sú podľa odsekov 2 a 3 zodpovední za škodu spôsobenú spracúvaním osobných údajov, za škodu zodpovedajú spoločne a nerozdielne.
- Ak prevádzkovateľ alebo sprostredkovateľ v súlade s odsekom 4 uhradil náhradu škody v plnej výške, má právo žiadať od ostatných prevádzkovateľov alebo sprostredkovateľov zapojených do toho istého spracúvania osobných údajov tú časť náhrady škody, ktorá zodpovedá ich podielu zodpovednosti za škodu za podmienok ustanovených v odseku

GDPR

BEZPEČNOSŤ OSOBNÝCH ÚDAJOV 1/3

Bezpečnosť spracúvania

- Prevádzkovateľ a sprostredkovateľ sú povinní prijať so zreteľom na najnovšie poznatky, na náklady na vykonanie opatrení, na povahu, rozsah, kontext a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzických osôb primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej tomuto riziku, pričom uvedené opatrenia môžu zahŕňať najmä

- a) pseudonymizáciu a šifrovanie osobných údajov,
- b) zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov,
- c) proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu,
- d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.

GDPR

BEZPEČNOSŤ OSOBNÝCH ÚDAJOV 2/3

Pri posudzovaní primeranej úrovne bezpečnosti sa prihliada na riziká, ktoré predstavuje spracúvanie osobných údajov

- najmä náhodné zničenie alebo nezákonné zničenie, strata, zmena alebo neoprávnené poskytnutie prenášaných osobných údajov, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo neoprávnený prístup k takýmto osobným údajom.

GDPR

BEZPEČNOSŤ OSOBNÝCH ÚDAJOV 3/3

Súlad s požiadavkami uvedenými v odseku 1 možno preukázať schváleným kódexom správania podľa § 85 alebo certifikátom podľa § 86. (interná smernica)

Prevádzkovateľ a sprostredkovateľ sú povinní zabezpečiť, aby fyzická osoba konajúca za prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, spracúvala tieto údaje len na základe pokynov prevádzkovateľa alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

GDPR

Oznámenie porušenia ochrany osobných údajov úradu 1/3

- Prevádzkovateľ je povinný oznámiť úradu porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o ňom dozvedel; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby.
- Ak prevádzkovateľ nesplní oznamovaciu povinnosť podľa odseku 1, musí zmeškanie lehoty zdôvodniť.
- Sprostredkovateľ je povinný oznámiť prevádzkovateľovi porušenie ochrany osobných údajov bez zbytočného odkladu po tom, ako sa o ňom dozvedel.

GDPR

Oznámenie porušenia ochrany osobných údajov úradu 2/3

Oznámenie podľa musí obsahovať najmä

- a) opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
- b) kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
- c) opis pravdepodobných následkov porušenia ochrany osobných údajov,
- d) opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.

GDPR

Oznámenie porušenia ochrany osobných údajov úradu 3/3

Prevádzkovateľ je povinný zdokumentovať každý prípad porušenia ochrany osobných údajov podľa odseku vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

GDPR

Oznámenie porušenia ochrany osobných údajov DO

Oznámenie porušenia ochrany osobných údajov dotknutej osobe

- kontaktné údaje zodpovednej osoby, ak je určená,
- posúdenie vplyvu na ochranu osobných údajov
- ďalšie informácie, o ktoré úrad požiada.

GDPR

Zodpovedná osoba

Určenie zodpovednej osoby čl.37 – 122/2013

- Pôvodne určená a definovaná už v zákone č. 122/2013
- Zmena definície
- oblasti povinnosti ňou disponovať
- právna zodpovednosť právnickej osoby
- osobnostné predpoklady

GDPR

ZODPOVEDNÁ OSOBA

Určenie zodpovednej osoby čl.37 – FO/PO/Negatívne vymedzenie

- Negatívne vymedzenie – zodpovednou osobou nemôže byť osoba ktorá by sa dostala pri výkone činnosti do konfliktu záujmu (štatutár, podnikateľ, majiteľ spoločnosti, konateľ)
- Zodpovednou osobou môže byť právnická osoba
- Právnická osoba musí poveriť FO v rámci vlastnej štruktúry
- Určenie tejto osoby musí byť súčasťou zmluvného vzťahu 2 PO
- Zodpovednou osobou môže byť fyzická osoba

GDPR

ZODPOVEDNÁ OSOBA

Určenie zodpovednej osoby čl.37 – zodpovedná osoba –

Osobnostné a kvalifikačné predpoklady :

- znalosť legislatívy na úrovni únie
- Znalosť interných procesov
- Znalosť problematiky riadenia rizík
- Znalosť bezpečnosti informačných systémov
- Znalosti napr. v oblasti bankového sektora

GDPR

ZODPOVEDNÁ OSOBA

Určenie zodpovednej osoby čl.37 – právna zodpovednosť zodpovednej osoby

- Zabezpečuje pozíciu Garanta
- Poverenie zodpovednej osoby **NEZNAMENÁ** zbavenie zodpovednosti prevádzkovateľa alebo sprostredkovateľa
- Účelom nie je nieť bremeno zodpovednosti ale pomáhať s odbornou starostlivosťou a poradenstvom v oblasti GDPR

GDPR

ZODPOVEDNÁ OSOBA

Určenie zodpovednej osoby čl.37 – Ľahká dostupnosť (pre viac subjektov)

- V prípade zastihnuteľnosti môže zastupovať viacero spoločností
- Možnosť zastihnúť osobne danú osobu
- Telefonicky
- Emailom
- Osobne

GDPR

ZODPOVEDNÁ OSOBA

Určenie zodpovednej osoby čl.37 – ohlasovanie

- Kontaktné údaje na zodpovednú osobu musia byť zverejnené na internetovej stránke spoločnosti ako aj oznámené úradu
- Na zverejnenie postačí uviesť telefónne číslo respektíve emailovú adresu (z.osoba@mail.sk)

GDPR

ZODPOVEDNÁ OSOBA

Určenie zodpovednej osoby čl.37 - úlohy v spoločnosti

- Poskytovanie poradenstva zamestnancov
- Dohliadanie na dodržiavanie a implementáciu GDPR do interných smerníc
- Kontaktná osoba smerom do vnútra spoločnosti
- Kontaktná osoba smerom k orgánom činným v oblasti ochrany osobných údajov

GDPR

ZODPOVEDNÁ OSOBA

Určenie zodpovednej osoby čl.37 – rozpor v legislatíve

- Nepodlieha nikomu v spoločnosti s výnimkou najvyššieho vedenia spoločnosti
- **Rozpor smernice** a SK zákonnej úpravy (The data protection officer shall directly report...)

GDPR

ZODPOVEDNÁ OSOBA

Určenie zodpovednej osoby čl.37 – definícia potreby ustanovenia zodpovednej osoby

- Pozitívne vymedzenie
- Negatívne vymedzenie
- **Neurčité vymedzenie – určené auditom**

GDPR

ZODPOVEDNÁ OSOBA

Určenie zodpovednej osoby čl.37

1. Prevádzkovateľ a sprostredkovateľ určia zodpovednú osobu v každom prípade ak
 - a) Spracúvanie vykonáva orgán verejnej moci alebo verejnoprávny subjekt s výnimkou súdov pri výkone ich súdnej právomoci
 - b) **Hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie**, ktoré vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú **pravidelné a systematické monitorovanie** dotknutých osôb vo veľkom rozsahu alebo (napr. prevádzkovatelia GPS modulov)

GDPR

ZODPOVEDNÁ OSOBA

c) Hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií údajov podľa článku 9 vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10 (spracovanie big data)

GDPR

ZODPOVEDNÁ OSOBA

Určenie zodpovednej osoby čl.37 – b) hlavné činnosti

- Predmetom činnosti je spracovanie dát v primárnych predmetoch a cieľoch podnikania
- Rozumejú sa nimi operácie ktoré sú nevyhnutné na dosiahnutie cieľa podnikania
- Spracovanie osobných údajov tvorí neoddeliteľnú súčasť

GDPR

ZODPOVEDNÁ OSOBA

Určenie zodpovednej osoby čl.37 – c) veľkom rozsahu

- Veľký rozsah sa dotýka veľkého množstva dát z pohľadu demografie / geografie / rozsahu dotknutých osôb
- Spracovanie big data (telefónne spoločnosti, banky, IT spoločnosti)