












GDPR (General Data Protection Regulation) – Ochrana osobných údajov

Ing. Oľga Bajnoková – Factiso
28.01.2022

Čo sú osobné údaje?



	Meno
	Adresa
	Lokalizácia
	Online identifikátor
	Zdravotné informácie
	Príjem
	Kultúrny profil
	a viac

ZBER UKLADANIE POUŽÍVANIE ÚDAJOV?

Musíte dodržiavať pravidlá.

Spracovanie údajov pre iné spoločnosti?
Toto sa dotýka aj vás.

Obsah :

- **Právny rámec - legislatíva**
- **Hlavné zmeny podľa GDPR**
- **Obsahový rámec - pojmy**



Právny rámec - Legislatíva



Účinné od  mája 2018

- **GDPR (General Data Protection Regulation)** - skratka **Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679** z 27.apríla o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica č. 95/46/ES (ďalej len GDPR)
- s **účinnosťou od 25. mája 2018** sa na území členských štátov EÚ začne uplatňovať jednotný režim ochrany osobných údajov
- toto nariadenie prináša **jednotnú právnu ochranu osobných údajov v členských štátoch EÚ**, ale aj zjednodušenie pravidiel spracúvania osobných údajov pre prevádzkovateľov, sprostredkovateľov
- **Zákon č. 18/2018 Z. z., Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov** spresňuje a implementuje požiadavky GDPR v našich vnútroštátnych predpisoch a vymedzuje rozsah osobných údajov, ktoré je prevádzkovateľ (ako zamestnávateľ) oprávnený poskytovať alebo zverejniť, ak je to potrebné v súvislosti s plnením pracovných povinností zamestnanca

Hlavné zmeny

- Nariadenie **zavádza nové pojmy** ako pseudonymizácia , profilovanie, genetický údaj a podobne
- **Rozširuje osobné údaje** o : IP adresy, cookies, RFID, e –mailové adresy, lokalizačné údaje a pod.
- Zavádza **osobitnú ochranu** osobných údajov **detí**
- Rozširuje **povinnosti** a zodpovednosti **sprostredkovateľa**
- Zavádza oznamovaciu povinnosť voči dotknutým osobám a voči Úradu na ochranu osobných údajov (**hlásenie do 72 hodín**)
- Právo na prenosnosť osobných údajov
- Právo **byť informovaný** o všetkých osobných údajov spracúvaných u prevádzkovateľa
- Právo na **opravu nesprávnych** osobných údajov
- Právo **na zabudnutie – vymazanie** osobných údajov

Obsahový rámec - Osobný údaj



Osobný údaj (OÚ) - každá informácia o identifikovanej či identifikovateľnej fyzickej osobe.

Identifikovateľnú fyzickú osobou je **priamo** či **nepriamo** možné identifikovať pomocou určitej informácie alebo kombinácií informácie. Identifikácia môže nastať rôznym spôsobom, nie vždy iba podľa mena, priezviska, adresy a dátumu narodenia, ale aj napr. kódom, ktorý má zamestnanec pridelený, alebo IP adresou.

Príklady kategórií najčastejšie využívaných osobných údajov:

- identifikačný údaj (meno a priezvisko, dátum narodenia / rodné číslo, číslo zamestnanca);
- kontaktný údaj (telefónne číslo, email, adresa);
- lokalizačný údaj (GPS z aut, použitie mobilného zariadenia);
- údaje o správaní v on-line prostredí (cookies, IP adresy);
- údaje o osobných a finančných pomeroch (ekonomická, kultúrna, spoločenská identita);
- osobitné kategórie OÚ.

Osobitné kategórie OÚ (citlivé údaje) - je nutné s nimi pracovať so zvýšenou opatrnosťou – napríklad mať tieto údaje v systéme evidované oddelene od iných údajov.

- Rasový alebo etnický pôvod
- Politické názory, náboženské alebo filozofické vyznanie alebo presvedčenie
- Členstvo v odborových organizáciách
- Genetické údaje
- Údaje týkajúce sa zdravia, sexuálneho života, sexuálnej orientácie
- Osobné údaje týkajúce sa uznania viny za trestné činy a priestupky



Obsahový rámec - pojmy



spracúvaním osobných údajov spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súborami osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami,



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,



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,



online identifikátorom identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiodrekvenčná 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,




Obsahový rámec - pojmy

 **dotknutou osobou** každá fyzická osoba, ktorej osobné údaje sa spracúvajú,

 **prevádzkovateľom** každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov,

 **sprostredkovateľom** každý, kto spracúva osobné údaje v mene prevádzkovateľa,

 **prijemcom** 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,



Čo všetko je podľa GDPR spracovanie osobných údajov?



Spracovanie osobných údajov označuje akúkoľvek aktivitu, alebo súbor aktivít, ktorú správca alebo spracovateľ uskutočňuje s osobnými údajmi, či už sa jedná o zhromažďovanie, uloženie, prehliadanie, štruktúrovanie, editácia, vyhľadávanie, odosielanie, vymazanie a pod. Ide o aktivitu, ktorá je prevádzaná systematicky a za jasne stanoveným **účelom**.

GDPR definuje zásady, ktorými je nutné sa pri spracovaní OÚ riadiť.

- **Účel spracovania** - určuje **dôvod**, pre ktorý sú osobné údaje spracovávané a určuje, čo sa s nimi bude diať.
Nesmie sa spracovávať žiadny osobný údaj, ak nemá identifikovaný svoj účel spracovania !

- **Právny titul** - naznačuje **druh oprávnenia**, na základe ktorého spracovávame osobné údaje.
GDPR rozlišuje celkom **šesť typov** právnych titulov spracovania osobných údajov, kedy **najpodstatnejšie** sú **tieto štyri**:



Nutnosť pre plnenie zmluvy

- Bankové spojenie na zamestnanca vyplnené v zamestnaneckej zmluve za účelom zasielania mzdy.
- Kontaktné údaje klienta pre zasielanie faktúr za poskytované služby.



Oprávnený záujem

- Nahrávanie pohybu zamestnancov v areáli kamerovým systémom.
- Zasielanie letákov newslettera existujúcim zákazníkom.



Nutnosť pre plnenie právnej povinnosti

- Informácie, ktoré sú poskytované pre plnenie zákonom určených povinností – napr. dáta poskytované finančným audítorom, alebo zdravotným poisťovniam.



Súhlas udelený subjektom OÚ

- Zasielanie marketingových oznamov návštevníkom webových stránok.
- Zverejnenie informácií o výhercoch súťaže na webovej stránke spoločnosti.

Zásady spracovania osobných údajov podľa GDPR



Zásady spracovania možno označiť za základné stavebné kamene nariadenia GDPR. Ide o súhrn zásad, ktoré musia byť pri spracovaní osobných údajov **vždy dodržiavané !** Vymedzenie, resp. dodržiavanie týchto zásad, je zásadné – GDPR určuje **zodpovednosť prevádzkovateľa za dodržiavanie týchto zásad** a zároveň povinnosť dodržiavania týchto zásad **adekvátnym spôsobom doložiť**.

Pri každom osobnom údaji potrebujeme poznať legitímny účel, pre ktorý ho použijeme. Osobné údaje nesmú byť spracované nezlučiteľným spôsobom za týmto účelom.

Účelnosť



Subjekt poskytujúci údaje je o spracovaní svojich dát informovaný bezodkladne, zrozumiteľne a nie je s nimi nakladané inak, než ako je uvedené v Informačnom memorande. Informácie o spracovaní OÚ sú najviac subjektom ľahko prístupné.

Zákonnosť, korektnosť a transparentnosť



Je možné zhromažďovať iba tie údaje, ktoré nutne potrebujeme pre daný účel. Nie je možné zhromažďovať osobné údaje subjektov len preto, aby sa mohli „niekedy hodiť“.

Minimalizácia



Presnosť



Integrita a dôvernosť

Osobné údaje subjektov je nutné vhodnými spôsobom ochrániť proti zneužitiu, alebo znehodnoteniu. Narušenie bezpečnosti osobných údajov je potrebné hlásiť dozorujúcemu orgánu do 72 hodín.



Nevyhnutná doba uloženia

Údaje musíme evidovať v systéme bez chyb, preklepov a v rovnakom formáte (napr. s diakritikou) a podľa potreby ich aktualizovať. Fyzické dokumenty je potrebné uschovať v čitateľnej podobe.

Všetky osobné údaje môžeme spracovať iba po nevyhnutnú dobu. Po uplynutí tejto doby je nutné údaje anonymizovať, alebo zmazať. Žiadne údaje nemôžeme držať tzv. „navždy“

Základné pojmy v GDPR



Čo je Osobný údaj v zmysle GDPR?

Osobný údaj je akákoľvek informácia o identifikovanej, alebo identifikovateľnej fyzickej osobe. Identifikovateľnou fyzickou osobou je možné priamo alebo nepriamo identifikovať pomocou určitej informácie alebo jej kombinácii. Napríklad: meno, pohlavie, vek, dátum narodenia IP adresa, fotografický záznam, e-mailová adresa, telefón apod.



Čo znamená Spracovanie osobných údajov podľa GDPR?

Spracovaním je myslená každá aktivita s údajmi, ako je zhromažďovanie, uloženie, prehliadanie, editácia, vyhľadávanie, odosielanie, vymazávanie, a pod., ktorá je robená systematicky za určitým cieľom.



Aké máme právne tituly pre spracovanie osobných údajov?

Právny titul je druh oprávnenia, na základe ktorého spoločnosť spracováva osobné údaje. GDPR identifikuje tieto : nevyhnutnosť pre plnenie zmluvy, nevyhnutnosť pre splnenie právnej povinnosti, oprávnený záujem správcu alebo tretej osoby, súhlas subjektu údajov, ochrana životne dôležitých záujmov subjektu údajov a verejný záujem alebo výkon verejnej moci.



Kto je subjekt údajov?

Subjekt údajov predstavuje fyzickú osobu (vrátane FO podnikajúcu), k nej sa osobné údaje vzťahujú. Subjekt údajov vždy nutne informujeme o tom, že jeho osobné údaje sú spracované a to jasným a zrozumiteľným jazykom v okamihu začatia spracovania osobných údajov.



Čo sa rozumie pod pojmom „účel spracovania“?

Účel spracovania je dôvod, pre ktorý sú osobné údaje spracovávané. Určuje čo sa bude diať s osobnými údajmi pri spracovaní.

Data Protection Officer (DPO)

= **DPO**, alebo **Zodpovedná osoba pre ochranu osobných údajov**, je novo zavedená funkcia, ktorú GDPR prináša. **DPO** bude plniť funkciu nezávislého pomocníka, alebo koordinátora ochrany osobných údajov u príslušného správcu alebo spracovateľa a súčasne funkciu akéhosi kontaktného bodu, pre jeho komunikáciu s dozornými úradmi (**Úrad na ochranu osobných údajov**).

Hlavnými úlohami Zodpovednej osoby pre ochranu osobných údajov (DPO) :

- Monitoruje súlad pri spracovaní s všeobecným nariadením a ďalšími predpismi.
- Poskytuje informácie dotýkajúcich sa GDPR v danej spoločnosti.
- Poskytuje na vyžiadanie poradenstvo, pokiaľ ide o posúdenie vplyvu na ochranu osobných údajov.
- Spolupracuje s Úradom pre ochranu osobných údajov.
- Podáva hlásenie dozornému orgánu v prípade úniku osobných údajov subjektu.
- Pôsobí ako kontaktná **osoba**.
- Zodpovedná osoba (DPO) môže plniť aj iné úlohy, ale pri ich plnení sa nesmie dostať do stretu záujmu s funkciou DPO.



Aké sú moje práva prístupu k údajov?

Dotknutá osoba má právo kedykoľvek vyžadovať :

- *potvrdenie*, či sú alebo nie sú osobné údaje o nej spracúvané,
- *informácie o spracúvaní osobných údajov v rozsahu :*
identifikačné údaje prevádzkovateľa a sprostredkovateľa, ak ho prevádzkovateľ má, zoznam osobných údajov a účel ich spracúvania, právny základ spracúvania osobných údajov ako aj informácie, či a komu sú osobné údaje poskytované, sprístupňované, prenášané a zverejňované,
- *informácie o zdroji*, z ktorého prevádzkovateľ získal jej osobné údaje na spracúvanie,
- *zoznam jej osobných údajov*, ktoré sú predmetom spracúvania,
- *opravu alebo likvidáciu svojich nesprávnych, neúplných alebo neaktuálnych osobných údajov*, ktoré sú predmetom spracúvania,
- *likvidáciu jej osobných údajov, ktorých účel spracúvania sa skončil*; ak dotknutá osoba poskytla prevádzkovateľovi svoje úradné doklady (originál/fotokópia), môže požiadať o ich vrátenie,
- *likvidáciu jej osobných údajov*, ak došlo k porušeniu zákona pri ich spracúvaní,
- *blokovanie jej osobných údajov z dôvodu odvolania súhlasu pred uplynutím času jeho platnosti*, ak prevádzkovateľ spracúva osobné údaje na základe súhlasu dotknutej osoby.



Čo musí urobiť vaša spoločnosť

Chrániť práva ľudí, ktorí vám poskytujú svoje údaje



Komunikácia

- Používajte bežný jazyk.
- Povedzte im, **kto** ste, keď žiadate o údaje.
- Uved'te, **prečo** spracováвате ich údaje, **ako** dlho budú uložené a **kto** ich dostane.



Prístup a prenosnosť

Umožnite ľuďom prístup k ich údajom a poskytnite ich inej spoločnosti.



Ochrana citlivých údajov

Použite dodatočné záruky pre informácie o zdraví, rase, sexuálnej orientácii, náboženstve a politickom presvedčení.

Čo musí urobiť vaša spoločnosť

Chrániť práva ľudí, ktorí vám poskytujú svoje údaje



Súhlas

Získajte jednoznačný súhlas so spracovaním údajov.

Zber údajov od detí pre sociálne médiá?
Skontrolujte vekový limit pre súhlas rodičov.



Upozornenia

Informujte ľudí o narušení údajov, ak pre nich existuje vážne riziko.



Odstránenie údajov

Dajte ľuďom „právo byť zabudnutý“. Vymažte ich osobné údaje, ak o to požiadajú, ale iba vtedy, ak sa tým neohrozí sloboda prejavu alebo možnosť preskúmania.



Prenos údajov mimo EÚ

Prijmite právne opatrenia pri prenose údajov do krajín, ktoré neschválili orgány EÚ.



Profílovanie

Ak na spracovanie žiadostí o právne záväzné dohody, ako sú napríklad pôžičky, používate profílovanie, musíte:

- informovať svojich zákazníkov,
- uistiť sa, že kontrolu procesu vykonáva osoba a nie stroj, ak bude žiadosť zamietnutá,
- ponúknuť žiadateľovi právo napadnúť rozhodnutie.

Chráňte údaje už v štádiu návrhu

Urobte záruky na ochranu údajov súčasťou svojich výrobkov a služieb už od prvých fáz vývoja.



Spracovanie údajov pre inú spoločnosť?

Uistite sa, že máte nenapadnuteľnú zmluvu, v ktorej sú uvedené povinnosti každej zmluvnej strany.

Vedenie evidencie

MSP musia viesť záznamy, len ak je spracovanie údajov

pravidelné

hrozbou pre práva a slobody osôb

také, pri ktorom sa zaobchádza s citlivými údajmi alebo trestnými záznamami



Evidencia by mala obsahovať:

- ✓ meno a kontaktné údaje podniku
- ✓ dôvody spracovania údajov
- ✓ opis kategórií dotknutých osôb a osobných údajov
- ✓ kategórie organizácií, ktoré dostávajú údaje
- ✓ prenos údajov do inej krajiny alebo organizácie
- ✓ lehotu na odstránenie údajov, ak je to možné
- ✓ opis bezpečnostných opatrení použitých pri spracovaní, ak je to možné

Predpokladajte na základe posúdení vplyvu

Posúdenia vplyvu môžu byť potrebné pre **VYSOKORIZIKOVÉ** spracovanie.



Náklady na nesplnenie povinností

Váš miestny orgán na ochranu údajov dohliada na dodržiavanie; jeho práca je koordinovaná na úrovni EÚ. Cena za porušenie pravidiel môže byť vysoká.



10 Príkazov GDPR pre zamestnancov

1. ZABEZPEČTE SI PRACOVISKO

Dbajte, aby v dobe Vašej neprítomnosti nemali prístup k fyzickým alebo elektronickým dokumentom nepovolane osoby. Aj pri krátkodobom opustení pracoviska uzamknite PC (stlačením Win +L), ak je to možné uzamknite kanceláriu.

2. MAJTE SVOJE DOKUMENTY POD KONTROLOU

Nenechávajte dokumenty s OÚ v tlačiarni, kopírke. Dokumenty ukladajte na určené miesta (do skrine, zásuviek a pod.). Nenechávajte PC, tablety a mobily v aute bez dozoru.

3. DODRŽIAVAJTE ZÁSADY INFORMAČNEJ A KYBERNETICKEJ BEZPEČNOSTI

Pri práci s elektronickými dokumentami dodržiavajte pokyny a odporúčania s ktorými ste boli poučení, nikdy nezdieľajte prístupové heslá do PC a iných informačných systémov. Heslo poznačené na papieri neuchovávajte v blízkosti PC alebo monitora.

10 Príkazov GDPR pre zamestnancov

4. KOMUNIKUJTE BEZPEČNE

OÚ posielajte výlučne cez schválené komunikačné kanály. Dokumenty s osobnými údajmi nikdy neukladajte na verejné úložisko (uložto, dropbox a pod.) a neposielajte ich prostredníctvom súkromného e-mailu.

5. INFORMUJTE SA O ÚČELOCH SPRACÚVANIA OSOBNÝCH ÚDAJOV

Majte na pamäti, že zamestnávateľ (teda aj Vy) ste oprávnený spracúvať len tie OÚ, ktoré sú potrebné pre dosiahnutie stanoveného účelu spracovania. Je dôležité vedieť, s akými OÚ ste oprávnený pracovať.

6. MINIMALIZUJTE ROZSAH A DOBU SPRACOVANIA OÚ

Pamätajte, že OÚ je možné spracúvať len v nevyhnutnom rozsahu a po nevyhnutne potrebujú dobu. Pokiaľ máte alebo získate prístup k OÚ, ktoré nepotrebujete, ohláste túto skutočnosť ihneď zodpovednej osobe/konateľovi a dohodnite si potrebné opatrenia.

7. BEZPEČNOSTNÉ INCIDENTY OKAMŽITE HLÁSTE

Pokiaľ dôjde k strate, znehodnoteniu, zničeniu, neoprávnenému prístupu k OÚ, oznámte ihneď túto skutočnosť zodpovednej osobe/ konateľovi.

10 Príkazov GDPR pre zamestnancov

8. PREHLBUJTE SVOJE VEDOMOSTI

Dôkladne sa oboznámte s internými predpismi, smernicami týkajúcimi sa OÚ, zúčastnite sa potrebných školení

9. PRISPIEVAJTE K ZLEPŠENIU OCHRANY OSOBNÝCH ÚDAJOV

Ak máte akékoľvek podnety, ako by bolo možné zlepšiť OOÚ, oznámte ich zodpovednej osobe / konateľovi alebo nadriadenému. Nikto nemá lepší prehľad o Vašom pracovisku a vykonávaných činnostiach než Vy.

10. NEBOJTE SA OTÁZOK

Ak nie ste si istý, ako postupovať v zabezpečení OOÚ obráťte sa zodpovednú osobu, ktorá Vám odporučí ako postupovať.

Ďakujem !

