

GDPR (General Data Protection Regulation)

OCHRANA OSOBNÍCH ÚDAJŮ OD 25. 5. 2018

GDPR je 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 s účinností od 25. května 2018 (dále jen „Nařízení“). Je platné pro všechny členské státy EU i bez zapracování do národní legislativy (na rozdíl od směrnice). Nařízení v tomto směru nahrazuje dosud platný český zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Předpis (úprava zákona 101), který zapracuje nové povinnosti vyplývající z Nařízení do českého právního řádu, prochází v současné době schvalovacím řízením Parlamentu České republiky a není tedy dosud schválen.

Smyslem Nařízení je ochránit data fyzických osob před možným zneužitím na všech úrovních – shromažďování, zpracování, ukládání, předávání,...

ZÁKLADNÍ POJMY

- **Osobní údaje**
 - **Osobní údaje** jsou **veškeré informace**, které se vztahují k již **identifikované** osobě a pomocí nichž lze danou osobu identifikovat (identifikovatelná osoba)
 - Dělení:
 - **Obecné:**
 - Jméno
 - Datum narození
 - Pohlaví
 - Osobní stav
 - Občanství
 - Fotografie
 - IP adresa
 - **Organizační**
 - Osobní nebo pracovní adresa
 - Telefonní čísla
 - E-mailové adresy
 - Identifikační čísla vydaná státem
 - **Zvláštní kategorie**
 - Citlivé
 - Genetické
 - Biometrické
- **Zvláštní kategorie a upřesnění**
 - **Citlivé údaje**
 - Zdravotní stav
 - Sexuální orientace

- Rasový nebo etnický původ
 - Politické názory a angažovanost
 - Náboženství a víra
 - Členství v odborech
- **Genetické údaje**
 - Analýzy biologických vzorků
 - Zděděné nebo získané genetické charakteristiky
- **Biometrické údaje**
 - Fyzické, fyziologické nebo behaviorální charakteristiky
 - Např. otisky prstů, fotografie obličeje nebo podpis!!
- Nevztahuje se na zesnulé osoby
 - Nevztahuje se na anonymizované údaje, ale vztahuje se na šifrované údaje (existuje možnost dešifrování a někdo musí znát způsob a klíč)
 - Nevztahuje se na fyzickou osobu v rámci činností osobní povahy, bez souvislosti s profesní nebo obchodní činností, např. seznam kontaktů v telefonu
- **Subjekt**
 - Fyzická osoba (dále jen „FO“) ve všech významech, tj. soukromá „privátní“ osoba i OSVČ (obchodní partner, zaměstnanec,...)
 - Pro potřeby spolků se jedná zejména o **člena klubu**
- **Správce dat**
 - OSVČ nebo právnická osoba, která při a pro své činnosti zpracovává údaje rezidentů EU
 - Ve smyslu Nařízení je správcem dat **spolek** (dále jen „správce“)
- **Zpracovatel dat**
 - Zpracovává osobní údaje pro správce
 - Jedná se o fyzickou nebo právnickou osobu, orgán veřejné moci, agenturu
- **Příjemce**
 - Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty
- **DPO**
 - Pověřenec pro ochranu osobních údajů
 - Jedná se kontaktní zodpovědnou osobu za agendu GDPR
- **Úřad pro ochranu osobních údajů (ÚOOÚ)**
 - Regulátor i pro GDPR
 - Nové další kompetence a pravomoci
 - Částečně bude podřízen Evropskému sboru pro ochranu osobních údajů (EDPB)
- **Databáze/evidence**
 - Jakýkoli strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií,
 - Může být centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska
- **Anonymizace**

- Proces, který znemožní k datům přiřadit konkrétní subjekt
- Anonymní údaj je takový, který nelze vztáhnout k určitému nebo určenému subjektu
- **Pseudonymizace**
 - Proces, který zachová vazbu na subjekt, ale „odosobní“ ji
 - Je to takové zpracování osobních údajů, že již nemohou být přiřazeny konkrétnímu subjektu bez použití dodatečných informací
- **Zpracování dat (osobních údajů)**
 - Jakákoli operace s osobními údaji
 - Patří sem: shromáždění, zaznamenání, uložení, jakékoli použití, nahlédnutí, vyhledání, omezení, uspořádání, seřazení, strukturování či zkombinování, jakékoli zpřístupnění, šíření, změna, přizpůsobení, výmaz či zničení

Základní principy zpracování osobních údajů

- **Zákonnost, spravedlnost a transparentnost vůči subjektu dat**
 - Správce musí zpracovávat data minimálně na základě alespoň jednoho právního důvodu dle Nařízení (čl. 6 nebo čl. 9 Nařízení), zpracování dat je zákonné pouze za předpokladu, že:
 - Subjekt udělil souhlas se zpracováním, ***udělení souhlasu se zpracováním je právem nikoli povinností!!!***
 - Souhlas nelze předpokládat (např. předvyplněním zaškrtnutí)
 - Je nezbytné pro přípravu nebo plnění smlouvy – minimální platnost po dobu trvání smlouvy a následného dotčeného období
 - Je nezbytné pro splnění právní povinnosti správce
 - Je nezbytné pro ochranu životně důležitých zájmů subjektu nebo jiné FO – typické jsou zdravotní údaje, alergie,... (např. soustředění, tábory...)
 - Je prováděno ve veřejném zájmu nebo při výkonu veřejné moci
 - Je nezbytné pro účely oprávněného zájmu správce (či třetí strany) – nesmí být dotčena základní práva a svobody subjektu, zejména v případě dětí
- **Pravidla evidence osobních údajů**
 - Dle Nařízení mají povinnost vést záznamy o zpracování osobních údajů organizace, které mají více než 250 zaměstnanců
 - Správce nebo zpracovatel je ovšem povinen vést záznamy o zpracování, které (jejichž):
 - Představují riziko pro práva a svobody subjektů údajů
 - Zpracování není příležitostné
 - Zahrnují zpracování zvláštních kategorií údajů
 - **Pro spolky je podstatné, že zpracování osobních údajů (vedení členské základny) není příležitostné, a proto by klub měl vést záznamy o zpracování údajů**
 - Záznamy o vedení musí dle Nařízení obsahovat minimálně tyto informace:
 - **Kontaktní údaje o správci**
 - **Účel zpracování osobních údajů** – stručný popis důvodu zpracování konkrétního údaje
 - **Kategorie subjektů a druh shromažďovaných osobních údajů** – např. zaměstnanci, členové, zákazníci, jméno a příjmení, adresa, kontakty, zdravotní stav...
 - **Kategorie příjemců** – jedná se o třetí strany, a to i pokud poskytujeme data do zahraničí
 - **Doba uchování osobní údajů** – např. po dobu trvání pracovního poměru, členství v klubu...

- **Externí a interní dokumentace** – jedná se o např. o pracovní smlouvy, dotazníky, přihlášky za člena... (externí), směrnice a předpisy správce, které přijal v souvislosti s GDPR (interní)
- **Shromáždění pro určité, výslovně vyjádřené a legitimní účely, minimalizace údajů, databáze**
 - Osobní údaje mohou být shromažďovány a zpracovávány pouze za jasně daným účelem
 - **Údaje shromážděné pro různé účely nelze libovolně propojovat, neboť pro každý účel bude jiný rozsah shromažďovaných údajů**
 - Při stanovení každého účelu shromažďování je nutné stanovit **rozsah osobních údajů**, které jsou **nezbytné (minimální možný rozsah) pro splnění uvedeného účelu**
 - Rozsah osobních údajů je nutné stanovit vždy předem, tedy při charakterizování účelu
 - **Konkrétně pro spolky:**
 - **Shromažďování osobních údajů, které souvisí se zabezpečením vlastní spolkové činnosti** – jedná se např. o pohlaví, v některých případech rodné číslo (členění do věkových kategorií, pojištění), kontaktní údaje, dosažené stupně kvalifikace rozhodčího... S poskytnutím těchto dalších osobních údajů je nutný souhlas subjektu.
 - **Subjekt vždy musí být informován o účelu a nutnosti poskytnout své osobní údaje**
 - Pozor na kopírování občanských průkazů nebo cestovních pasů – požadované údaje je lépe přepsat nebo pořídit šablonu na kopírování pouze požadovaných osobních údajů
 - Účel shromažďování osobních dat musí být charakterizován konkrétně, nelze pouze obecně
 - **U spolků ČMKU se předpokládají účely zpracování osobních údajů tyto:**
 - **Registrace členství ve spolku**
 - **Tvorba databáze členské základny a nakládání s ní** – nutný souhlas člena klubu
 - **Ostatní účely** – nutný souhlas člena klubu
- **Přesnost údajů a aktuálnost dat**
- **Omezení uložení**
 - Ukládat po nezbytně nutnou dobu vzhledem k účelu, pro který jsou osobní data používána
- **Integrita, zabezpečení a důvěrnost**
 - Zajistit, aby osobní data byly zpracovávány pouze odpovědnými osobami, zamezit jejich zneužití
 - Správce je povinen přijmout taková opatření, aby zamezil zneužití, odcizení, změně či ztrátě osobních dat
 - Nutné zamezit přístupu neoprávněných osob k databázím, nejlépe stanovit vždy jednu odpovědnou osobu, která bude mít ke všem databázím s osobními údaji přístup
 - **Při ochraně osobních údajů dodržovat následující pravidla:**
 - Veškerá data (písemná či na nosičích informací) chránit před volným přístupem neoprávněných osob
 - Písemné materiály uchovávat v uzamykatelných skříních a v uzamykatelných místnostech, platí i pro datové nosiče
 - Zodpovědná osoba (správce) může pověřit další oprávněné osoby k nakládání s osobními údaji, vždy pouze v přesně určeném rozsahu a ke konkrétnímu účelu
 - Server, na kterém jsou data uložena, musí být chráněn antivirovým systémem a firewallem proti internetovým útokům, server musí být umístěn v uzamykatelné skříně a v uzamykatelné místnosti
 - Databáze (soubory dat) musí být pravidelně zálohovány
 - PC zaheslovat jménem a heslem
 - Zaheslovat i adresáře s osobními údaji
 - Databáze na přenosných PC (notebook) zabezpečit zašifrováním
 - Všechny osoby, které přijdou do styku s osobními údaji (správce, pověřené osoby, zpracovatel) mají

povinnost mlčenlivosti

- K naplnění povinnosti zabezpečit osobní údaje je správně nutné přijmou **vnitřní (interní) směrnice a předpisy** pro nakládání s osobními údaji (oprávněné osoby, postupy a pravidla nakládání s osobními údaji ... viz popis výše)
- **Úprava při nakládání s fotografiemi** – k nakládání s nimi je potřeba souhlas subjektu, který může být poskytnut již při vyplňování přihlášky za člena klubu, pak se jedná pouze o nakládání za účelem informování o vlastní činnosti klubu, využití fotografií v souvislosti s marketingovou činností není povoleno
- **Kamerový systém** – samotné použití kamerového systému není považováno za zpracování osobních dat, tím se stává až v okamžiku, kdy dochází k pořizování záznamů záběrů z kamerového systému, v tomto případě je nutné stanovit účel pořizování dat (ochrana majetku a bezpečnosti a zdraví osob), nezasahovat nadměrně do soukromí subjektů (ne na toaletách, šatnách,...), určit lhůtu pro uchovávání záznamů, nosiče s daty adekvátně ochránit před zneužitím, subjekty musí být o použití kamerového systému informovány (informační tabule,...), zpracovat vnitřní směrnici o použití kamerového systému
- **Zpracování osobních údajů dětí mladších 15 let**
 - Nutný souhlas zákonného zástupce!!!, děti starší 15 let mohou udělit souhlas bez omezení
- **Vztah správce - zpracovatel**
 - Správce je primárně zodpovědná osoba za data a zpracovatel je najímám správcem
 - Vztah mezi správcem a zpracovatelem musí mít podobu **písemné smlouvy**, která obsahuje:
 - Předmět smlouvy
 - Dobu trvání
 - Povahu a účel zpracování
 - Typ zpracovávaných údajů (kategorie)
 - Povinnosti a práva správce a zpracovatele
 - Jedná se především o jakékoli zpracovatelské smlouvy – např. zpracování účetnictví, daňové poradenství, IT služby,...
 - Smlouva dále musí stanovit, že zpracovatel nepověří zpracováním osobních údajů dalšího zpracovatele bez předchozího souhlasu správce
 - Zpracovatel či jím pověřená další osoba musí dodržovat všechny zásady k ochraně osobních dat a musí se zavázat k dodržování interních předpisů správce (spolku) o ochraně osobních údajů

Základní práva subjektů

Správce je povinen informovat subjekt o zpracování osobních údajů, z tohoto také vyplývají základní práva subjektů:

- **Právo na informovanost (na přístup)**
 - Kontaktní údaje správce
 - Zda jsou údaje subjektu zpracovávány či nikoli
 - V jakém rozsahu (kategorie OÚ)
 - K jakému účelu
 - Příjemce osobních údajů
 - Na jakou dobu
 - Z jakého zdroje, pokud nejsou data poskytnuta samotným subjektem
 - Zda dochází k automatizovanému zpracování
 - Jak podat stížnost k ÚOOÚ

- **Právo na opravu**
 - Při podezření požádat o opravu dat a povinnost správce tuto opravu bez zbytečného odkladu zajistit
- **Právo být zapomenut**
 - Pokud pominul účel
 - Pokud subjekt odvolal souhlas
 - Pokud byly osobní údaje zpracovány protiprávně (např. bez souhlasu pokud je nutný)
 - Pokud není dán rodičovský souhlas se zpracováním osobních údajů dětí mladších 15 let
- **Právo na výmaz**
 - Rozšíření práva „být zapomenut“
 - Provedení přiměřených kroků (včetně technických opatření) k vymazání veškerých osobních údajů na všech místech – včetně záloh nebo při automatické obnově IT systémů
- **Omezení zpracování**
 - Alternativní řešení k právu „být vymazán“
 - Data budou dočasně nedostupná
 - Přenesení dat do separátního systému
 - Data budou pouze uložena, ale nebudou zpracovávána (např. při vznesení námitky do doby, než se prověří legitimnost zpracování)
- **Právo na přenositelnost údajů**
 - Má usnadnit přenos osobních údajů mezi správci
 - Pouze v případě, že zpracování je založeno na souhlasu nebo smlouvě a je prováděno automatizovaně
 - Nelze uplatnit při zpracování ve veřejném zájmu nebo při výkonu veřejné moci
 - Subjekt má právo získat své údaje ve strukturovaném, běžně používaném a strojově čitelném formátu, popř. správce má povinnost předat data novému správci
 - Formát není specifikován, předpokládá se XML nebo CSV
 - Očekává se výkladový materiál od WP29 – pracovní skupina Evropské komise složená ze zástupců dozorových úřadů členských zemí EU
- **Právo vznést námitku**
 - Výslovné upozornění subjektu vzhledem ke zpracování vlastních dat v konkrétní situaci
 - Požadavek „dokázat“ legálnost zpracování dat
 - Očekává se pozastavení zpracování do té doby, než se situace vyjasní

Správce dat má povinnost naplnit práva subjektů bez zbytečného odkladu, a to maximálně do 1 měsíce, v oprávněných případech a po předchozím informování subjektu až do 3 měsíců.

V případech, kdy nějaký subjekt svá práva zneužívá, může se správce bránit přiměřeným poplatkem (zneužití ovšem dokládá správce).

Pokud se jedná o zjevnou šikanu, může správce i odmítnout, v takovém případě se ovšem doporučuje předem situace konzultovat / nahlásit ÚOOÚ.

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

- **Hranice pro jmenování**

- Je povinný pro veřejné orgány (orgány veřejné moci nebo veřejné subjekty – obce, nemocnice, školy,...)
- Rozsáhlé a systematické monitorování fyzických osob
- Rozsáhlé zpracování citlivých dat

Povinnost, kdy jmenovat pověřence, není přesně definována, je závislá na účelu a rozsahu zpracování osobních údajů (např. počet subjektů, rozsah zpracovávaných dat, doba trvání...). Podle dostupných výkladů pro spolky tato povinnost nevyplývá.

- **Požadavky na pověřence**

- Znalosti v oblasti informačních technologií, práva
- Komunikační schopnosti a krizové řízení

- **Úkoly pověřence**

- Monitorování v souladu s Nařízením
- Řízení činnosti interní ochrany
- Provádění interních auditů
- Školení pracovníků ve zpracování dat

V těchto případech se jedná o pověřence, který musí být jmenován. Jak je již uvedeno výše, pro potřeby spolků se vyvozuje, že pověřenec v tomto rozsahu povinností jmenován být nemusí. **Doporučujeme však jmenovat osobu, která bude mít celý proces zpracování osobních údajů ve své gesci a zajistí vše zejména dle odst. 6 Základních principů zpracování osobních údajů, tzn. zajistit, aby k osobním údajům neměl přístup kdokoli a byla řádně zabezpečena.** Také to bude kontaktní osoba pro dozorový úřad – ÚOOÚ.

Prvotní analýza

Cílem analýzy je zodpovězení následujících otázek:

- Co sbírám
- Proč sbírám
- Kde ukládám
- Na jak dlouho
- Kdo má přístup
- Jak mám zabezpečeno
- Z titulu informací o zaměstnancích či členské základně
- Z titulu informací o obchodních partnerech

Výsledek analýzy:

- Výstup z analýzy by se měl porovnat s obecným nařízením GDPR a provést následující úkony:
 - Opatření:
 - Minimalizace dat
 - Obsahová – vymazat nelegitimní informace
 - Časová – vymazat informace, pro které pominul důvod
 - Úložiště - neduplikovat zbytečně údaje na více míst
 - Omezení přístupu (zpracování v širším významu)
 - Omezit přístup k datům osobám, které jej nepotřebují
 - I pro oprávněné osoby omezit zpřístupněná data
 - Omezit či zakázat přístup třetím stranám

- Zabezpečení dat
 - V listinné podobě
 - V elektronické podobě
- Dokumentace:
 - Popis stavu
 - Interní směrnice, smlouvy, dodatky
 - Prokazatelně seznámit dotčené osoby s tím, co musí, co smí a co nesmí
 - Bezpečnost
 - Zdokumentovat díry
 - Nastavit kontrolní mechanismy
 - Připravit postupy „Co se stane, když ...“
 - Kontrolní body a zpětná vazba

DOPORUČENÍ!!!

- Založit tzv. „šanon GDPR“
- Obsah:
 - Prvotní analýza, včetně datové mapy – viz příloha
 - Oficiální zpracovaná analýza – popis procesu s nakládáním (kdo nakládá, kde uloženo, hesla, jaké dodatky k již platným smlouvám, zda souhlasy se zpracováním osobních údajů a popřípadě k jakým údajům,...)
 - Správcovsko – zpracovatelské smlouvy (např. IT služby, účetní služby...)
 - Dodatky pracovních smluv – protokoly a poučení zaměstnanců
 - Souhlasy s fotkami - reportáže + dokumenty
 - Interní směrnice, např. jak nakládat s kamerovým systémem, nakládání s daty
 - Krizový plán
 - Vyhodnocení závažnosti bezpečnostních incidentů (např. zda nutné zašifrování dat)
 - Kontakt na ÚOOÚ
 - Plán kontrol zpracování dat – stačí 1x za rok