# 4 Ochrana osobních údajů

Ochrana fyzických osob v souvislosti se zpracováním osobních údajů patří mezi základní práva. Termín „GDPR“ resp. Zákon o ochraně osobních údajů, je stále známějším pojmem, avšak od doby jeho schválení vzniklo množství mýtů a polopravd, kvůli kterým mnozí lidé netuší co to vlastně je a v jakých případech se používá.

## 4.1 GDPR

Ve zkratce, GDPR je obecné nařízení Evropské Unie, které se věnuje ochraně osobních údajů a bylo přijato v roce 2016. Toto nařízení platí pro všechny členské státy a upravuje:

a) ochranu práv fyzických osob před neoprávněným zpracováním jejich osobních údajů,
b) práva, povinnosti a odpovědnost při zpracovávání osobních údajů fyzických osob,
c) postavení, působnost a organizaci Úřadu na ochranu osobních údajů České republiky (dále jen „úřad“).

### 4.1.1 Důležitost GDPR

Před samotným zavedením zákona GDPR byli občané jednotlivých států chráněni zákony, morálními kodexy a prohlášeními společností shromažďujících naše údaje. Po zavedení tohoto nařízení se nejen sjednotila, ale i zpřísnila legislativa pro celou EU, a zároveň se doplnily všechny chybějící zákony o ochraně osobních údajů na internetu.

Právě díky GDPR musí společnosti mnohem bezpečněji zacházet s našimi daty. Pod bezpečným zacházením můžeme rozumět, že daný provozovatel nesmí bezdůvodně předávat osobní údaje třetím osobám (firmám), případně je zveřejňovat bez našeho souhlasu. Možná to zní absurdně, ale ne tak dávno se daly na internetu legálně koupit databáze emailových adres a telefonních čísel (což využívali různí „prodejci bambusových ponožek“).

Dnes je již oficiálně takový postup protizákonný. Pokud někomu nedáte souhlas s tím, aby zveřejnil váš email nebo telefon, tak jej zveřejnit nesmí. Rovněž nemůže, bez vašeho souhlasu poskytnout vaše údaje třetím stranám (tzv. dalším firmám). Navíc, pokud udělíte svůj souhlas firmě, můžete jej kdykoli odvolat a firma musí vaše údaje smazat.

## 4.2 Osobní údaj

Pod osobním údajem rozumíme údaj týkající se identifikované fyzické osoby nebo identifikovatelné fyzické osoby, kterou lze identifikovat přímo nebo nepřímo zejména na

základě obecně použitelného identifikátoru, jiného identifikátoru. Jinými slovy jde o všechny dostupné informace, v rámci kterých můžeme jakýmkoli způsobem identifikovat konkrétní osobu.

Mezi nejznámější osobní údaje patří například demografické a geografické údaje, kterými jsou věk, pohlaví, národnost, místo bydliště a pod. Do osobních údajů však spadá i IP adresa zařízení a jeho poloha, jelikož v dnešní době lze konkrétní mobil (počítač), s vlastní IP adresou a polohou, spojit s osobou.

### 4.2.1 Zásady zpracování osobních údajů

Při zpracování osobních údajů musí být v první řadě dodrženy stanovené zásady.

1. **Zásada zákonnosti** – osobní údaje lze zpracovávat jen zákonným způsobem tak, aby nedošlo k porušení základních práv dotčené osoby.
2. **Zásada omezení účelu**- osobní údaje lze získat pouze pro **konkrétně určený, vysloveně uvedený a oprávněný účel**. Zároveň se údaje nesmějí dále zpracovávat způsobem jiným než je určen.
3. **Zásada minimalizace osobních údajů**- osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah daný účelem, pro který se zpracovávají.
4. **Zásada integrity a důvěrnosti –** osobní údaje musí být zpracovány prostřednictvím přiměřených technických a organizačních opatření, která zaručují primární bezpečnost včetně ochrany před neoprávněným zpracováním, náhodnou ztrátou, výmazem nebo poškozením osobních údajů.
5. **Zásada odpovědnosti –** Provozovatel je zodpovědný se dodržování základních základních zásad zpracování.

### 4.2.2 Zvláštní kategorie osobních údajů

Zákon zakazuje zpracování zvláštních kategorií osobních údajů, které odhalují rasový původ nebo etnický původ, politické názory, náboženskou víru filozofické přesvědčení, členství v odborových organizacích, genetické údaje, biometrické údaje, údaje týkající se zdraví nebo údaje týkající se sexuálního života nebo sexuální orientace fyzické osoby.

Tento zákaz zpracování zvláštních kategorií osobních údajů neplatí, pokud:

- dotyčná osoba (fyzická osoba) vyjádřila výslovný souhlas se zpracováním těchto osobních údajů
- zpracování je nezbytné pro ochranu života, zdraví nebo majetku dotčené osoby
- zpracování v rámci oprávněné činnosti občanské sdružení, nadace nebo nezisková organizace poskytující obecně prospěšné služby, politická strana nebo politické hnutí, odborová organizace, státem uznaná církev nebo náboženská společnost
- zpracování je nezbytné pro účel sociálního pojištění, sociálního zabezpečení policistů a vojáků, poskytování státních sociálních dávek, podpory sociálního začlenění fyzické osoby s těžkým zdravotním postižením do společnosti
- zpracování je nezbytné pro účel archivace, pro vědecký účel, pro účel historického výzkumu nebo pro statistický účel

***Případová studie***

*Ján Novotný je hlavním zakladatelem občanského sdružení, které v posledních letech velmi prosperuje. Díky svému růstu zvažuje nábor nových zaměstnanců. Po několika úspěšných pohovorech se rozhodne přijmout 3 uchazečky. V osobním dotazníku však žádá vyplnit kolonku týkající se zdraví daných osob. Porušil daný zaměstnavatel zákon GDPR nebo jednal v souladu se zákonem? Svou odpověď zdůvodni.*

*a) Ano, pan Novotný jednal v souladu se zákonem.*

..... .....

.....

*b) Ne, pan Novotný nejednal v souladu se zákonem.*

..... .....

.....

### 4.3 Práva subjektu údajů

Zákon GDPR vymezuje základní práva subjektu údajů a povinnosti provozovatele. K právům dotyčných osob patří:

- **Právo na opravu osobních údajů -** dotyčná osoba má právo na to, aby provozovatel bez zbytečného odkladu opravil nesprávné osobní údaje.

- **Právo na výmaz osobních údajů -** dotyčná osoba má právo na to, aby provozovatel bez zbytečného odkladu vymazal osobní údaje.
- **Právo na omezení zpracování osobních údajov-** dotknutá osoba má právo na to, aby provozovatel omezil zpracování osobních údajů.
- **Právo na přenosnost osobních údajů –** dotyčná osoba má právo získat osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu, které se jí týkají a které poskytla provozovateli, a zároveň má právo přenést tyto osobní údaje dalšímu provozovateli.
- **Právo na náhradu škody a odpovědnost**
- **Právo namítat zpracování osobních údajů**

### 4.4 Povinnosti provozovatele

- Provozovatel je povinen přijmout vhodná technická a organizační opatření k zajištění a prokázání toho, že zpracování osobních údajů se provádí v souladu s tímto zákonem.
- Provozovatel je povinen zavést přiměřené postupy ochrany osobních údajů ze strany provozovatele, je-li to vzhledem ke zpracovatelské činnosti přiměřené.
- Provozovatel je povinen zavést standardní ochranu osobních údajů, která spočívá v přijetí přiměřených technických a organizačních opatření k zajištění zpracování osobních údajů pouze pro konkrétní účel, minimalizaci množství získaných osobních údajů a rozsahu jejich zpracování, doby uchovávání a dostupnosti osobních údajů.
- Provozovatel je povinen pravidelně prověřovat trvání účelu zpracování osobních údajů a po jeho splnění bez zbytečného odkladu zajistit výmaz osobních údajů.
- Provozovatel je povinen zohlednit nejnovější poznatky ochrany osobních údajů.
- K prokázání splnění povinností, může provozovatel použít certifikát.

#### 4.4.1 Důležitá povinnost provozovatele webové stránky

Pokud daná osoba podniká na internetu a má webovou stránku, tak se na něj vztahuje GDPR nařízení. Povinností je proto upozornit návštěvníky stránky, že sbírá a zpracovává jejich osobní údaje (IP adresa, poloha apod.). Je proto povinností každé stránky mít platné prohlášení resp. poučení o ochraně a zpracování osobních údajů a poučení o cookies. Toto vše je obsaženo v dokumentu prohlášení o ochraně a zpracování osobních údajů, který musí mít umístěn na stránce.

Tento dokument musí popisovat způsob, jakým zacházíte s osobními údaji resp. jak je chráníte, musí obsahovat rozsah a podmínky zpracování, práva dotyčné osoby (např. právo na vymazání/omezení) a další náležitosti. Samozřejmě, musí být aktualizován podle platné legislativy a musí reflektovat všechny změny v této oblasti.

### 4.4.2 Výše pokuty v případě nesplnění

V případě, že provozovatel nedodrží tuto povinnost, může mu hrozit vysoké pokuty. Samozřejmě vše závisí na závažnosti porušení ochrany osobních údajů. Rozdíl je vnímán v první řadě, zda se jednalo o neaktualizovanou dokumentaci, nebo zda se záměrně prodávaly databáze dalším firmám. Udělené sankce se mohou pohybovat od stovek až po miliony eur. U velkých firem je strop sankcí stanoven jako 4% z celkového obratu společnosti.

*Zajímavost: Příkladem je pokuta pro leteckou společnost British Airways ve výši 204,4 milionu eur (1,5 % z celkového obratu v roce 2017), která je dosud historicky nejvyšší pokuta za porušení GDPR.*

## 4.5 Základní nařízení přijatá zavedením zákona

1. **Jednodušší přístup k vlastním osobním údajům-** více informací o tom, jak jsou osobní údaje zpracovávány, a tyto informace budou dostupné v jasné a srozumitelné podobě.
2. **Právo být informován o zneužití mých osobních údajů -** společnost a organizace, resp. provozovatel musí co nejdříve informovat vnitrostátní orgán dozoru o závažném narušení ochrany osobních údajů, aby mohli uživatelé přijmout vhodná opatření.
3. **Jasněji vymezené „právo být zapomenut“ -** pokud si fyzická osoba nepřeje, aby byly osobní údaje dále zpracovávány, a neexistuje-li žádný právní základ pro jejich uchovávání, budou tyto osobní údaje vymazány.
4. **Jedno kontaktní místo („one.stop.shop!“):** podniky komunikují s jedním kontrolním orgánem.

## 4.6 Instituce

- **Úřad na ochranu osobních údajů ČR**
- **Slovenská obchodní inspekce**
- **Společnost ochrany spotřebitelů**

**<u>Otázky a úkoly:</u>**

*1. Existovaly před zavedením zákona GDPR, zákony na ochranu osobních údajů?*

*2.V kterém roce schválili zákon GDPR a pro koho je platný?*

*3.Uveďte základní osobní údaje, které se běžně zpracovávají.*

*4.Uveďte alespoň 3 práva dotyčné osoby vyplývající ze zákona.*

*5. Vyjmenujte, pro které organizace se nevztahuje povinnost, která zakazuje zpracování zvláštních kategorií osobních údajů.*

*6. V jaké výši se pohybuje strop sankcí pro velké firmy, v případě porušení zákona GDPR?*

*7. V případě neaktualizování dokumentace dostane firma sankci ve stejné výši jako firma, která prodala databázi jiné firmě? Odpovězte ano/ne a svou odpověď zdůvodněte.*

*8. Uveďte, zda má dotyčná osoba právo na úpravu osobních údajů.*

*9.Vyjádřete svůj názor, jak byste reagovali a případně postupovali v případě, že by vaše osobní údaje byly zneužity.*

**Zdroje:**

[1] *GDPR-Vše, co potřebujete vědět.* [online]. [2020]. [citováno 31. 8. 2021]. dostupné na: https://pravoeshopov.sk/gdpr-vsetko-co-potrebujete-vedet/

[2] *Nařízení evropského parlamentu a rady EU.* [online]. [2016]. [citováno 31. 8. 2021]. dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32016R0679

[3] *Zákon č. 18/2018 Z. z.Zákon o ochraně osobních údajů ao změně a doplnění některých zákonů* [online]. [citováno 31. 8. 2021]. dostupné na: https://www.epi.cz/zz/2018-18