Podané ruce
na cestě ke svobodě

# General Data Protection Regulation (GDPR)

Nařízení (EU) 2016/679

**ZÁKLADNÍ INFORMACE**

pro zaměstnance společnosti, externí pracovníky a spolupracující dobrovolníky


Adresa: Společnost
Podané ruce o.p.s.
Hilleho 5, 602 00 Brno

T: +420 545 247 535
M: +420 777 916 285
E: info@podaneruce.cz

Bankovní spojení: Oberbank AG 2231107576/8040
DIČ: CZ60557621
IČO: 60557621

## GDPR - OBECNÁ DEFINICE

Obecné nařízení na ochranu osobních údajů neboli **GDPR (General Data Protection Regulation)** je dosud nejvíce uceleným souborem pravidel na ochranu dat na světě.

GDPR se dotýká každého, kdo shromažďuje nebo zpracovává osobní údaje Evropanů, včetně společností a institucí mimo území EU, které působí na evropském trhu.

Nařízení míří na firmy, instituce i jednotlivce, kteří zacházejí s osobními údaji zaměstnanců, zákazníků, klientů či dodavatelů, a to napříč segmenty a odvětvími. Zasáhne i ty, kteří sledují či analyzují chování uživatelů na webu, při používání aplikací nebo chytrých technologií. Cílem GDPR je chránit digitální práva občanů EU.
GDPR zavádí celou řadu nových pravidel. Jejich platnost a dodržování bude muset každý správce i zpracovatel osobních údajů prokazatelně doložit po celou dobu zpracování. Přibude mu tím velká administrativní zátěž, bude muset například dokumentovat, že zpracovává pouze ta data, která jsou ke konkrétnímu účelu nezbytná.

GDPR dává lidem, kterým údaje patří (těm říká subjekty údajů), do rukou nová práva. Kromě toho, že budou muset být o svých právech důkladně informováni, pak budou moci po správcích údajů vyžadovat něco, co doposud nemohli. Jde například o právo vznést námitku proti zpracování, kdy správce po takové námitce nebude moci údaje dále zpracovávat, nebude-li k tomu mít závažné, prokazatelné důvody; či o právo na přenositelnost osobních údajů od jednoho správce k druhému, jestliže jsou údaje zpracovávány automatizovaně. Žadatel by své osobní údaje měl v takovém případě získat ve strukturovaném, strojově čitelném formátu.

Zpracovatel bude muset ohlásit únik či ohrožení zabezpečení osobních dat Úřadu pro ochranu osobních údajů nejpozději do 72 hodin od okamžiku, kdy se o incidentu dozvěděl. V některých případech bude muset také informovat osoby a subjekty, kterých se únik týkal.

**Adresa:** Společnost
Podané ruce o.p.s.
Hilleho 5, 602 00 Brno

**T:** +420 545 247 535
**M:** +420 777 916 285
**E:** info@podaneruce.cz

**Bankovní spojení:** Oberbank AG 2231107576/8040
**DIČ:** CZ60557621
**IČO:** 60557621

## OSOBNÍ ÚDAJE

Osobní údaje jsou ve stávající směrnici z roku 1995 i v GDPR definovány jako veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě.

Mezi obecné osobní údaje řadíme jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresu a fotografický záznam. Vzhledem k tomu, že se GDPR vztahuje i na podnikající fyzické osoby, řadíme mezi osobní údaje i tzv. organizační údaje, kterými jsou například e-mailová adresa, telefonní číslo či různé identifikační údaje vydané státem.

Obecné nařízení věnuje speciální pozornost zpracování zvláštních kategorií osobních údajů, jimiž jsou údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení. Do kategorie citlivých údajů nařízení nově zahrnuje genetické, biometrické údaje a osobní údaje dětí. Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu, než je tomu u obecných údajů.

Genetickými údaji jsou osobní údaje týkající se zděděných nebo získaných genetických znaků určité fyzické osoby, které vyplývají z analýzy biologického vzorku dotčené fyzické osoby nebo z analýzy jiného prvku, která umožňuje získat rovnocenné informace. Mezi osobní údaje o zdravotním stavu by měly být zahrnuty veškeré údaje související se zdravotním stavem, které vypovídají o tělesném nebo dušením zdraví člověka.

Biometrickým údajem jsou osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňují jedinečnou identifikaci. Typickým biometrickým údajem je např. snímek obličeje, otisk prstu, ale podle poslední judikatury i podpis.

## PRÁVA OBČANŮ Z GDPR

Jedním z největších dopadů nařízení je výrazné posílení práv občanů neboli tzv. ***subjektů údajů.*** Těmito právy jsou zejména práva na přístup, opravu, výmaz, právo být zapomenut, právo na omezení zpracování, přenositelnost údajů a v neposlední řadě právo vznést námitku.

Příkladem práv na přístup je informace o zdravotním stavu subjektu, přístup k údajům ve své zdravotní dokumentaci, která obsahuje například informace o diagnóze, výsledky vyšetření, posudky ošetřujících lékařů a údaje o veškeré léčbě a provedených ošetřeních nebo zákrocích.

Každý občan tedy bude mít právo vědět a být informován zejména o tom, za jakým účelem se osobní údaje zpracovávají – znát období, po které budou údaje uchovávány, znát příjemce jeho osobních údajů, vědět, v čem spočívá logika automatizovaného zpracování osobních údajů a jaké mohou být důsledky takového zpracování přinejmenším v případech, kdy je zpracování založeno na profilování.

Naprosto novým právem podle GDPR je právo na to, aby správce bez zbytečného odkladu vymazal naše osobní údaje, pokud je dán jeden z těchto důvodů:

- Osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány.
- Občan odvolá souhlas, pokud je zpracování založeno na souhlasu a neexistuje žádný další právní důvod pro zpracování.
- Občan vznese námitku proti zpracování z důvodu oprávněných zájmů správce osobních údajů, jako je např. vedení záznamů o zaměstnancích.
- Osobní údaje byly zpracovány protiprávně.
- Pokud není dán rodičovský souhlas se zpracováním osobních údajů dětí.
- Právní povinnost stanovená právem Unie nebo členským státem.

Aby měl občan větší kontrolu nad svými údaji, měl by v případě, kdy se osobní údaje zpracovávají automatizovaně, mít též právo získat osobní údaje, které se ho týkají a jež poskytl správci, ve strukturovaném, běžně používaném, strojově čitelném formátu a předat je jinému správci. Vzhledem ke své povaze by toto právo nemělo být uplatňováno vůči správcům, kteří zpracovávají osobní údaje v rámci výkonu veřejné moci. Pokud se určitý soubor osobních údajů týká více než jednoho subjektu údajů, neměla by právem obdržet osobní údaje být dotčena práva a svobody jiných subjektů údajů podle tohoto nařízení.

**Adresa:** Společnost
Podané ruce o.p.s.
Hilleho 5, 602 00 Brno

**T:** +420 545 247 535
**M:** +420 777 916 285
**E:** info@podaneruce.cz

**Bankovní spojení:** Oberbank AG 2231107576/8040
**DIČ:** CZ60557621
**IČO:** 60557621

## ODPOVĚDNOST SPRÁVCE DAT

Nařízení nově zavádí princip tzv. zodpovědnosti, který spočívá v povinnosti správců a zpracovatelů údajů bez ohledu na jejich velikost nebo počet zaměstnanců zavést technická, organizační a procesní opatření za účelem prokázání souladu s principy GDPR. Uplatnění principu zodpovědnosti bude představovat pro podnikatele nemalé časové a finanční investice. Ty se budou týkat zejména těchto oblastí:

- implementace záměrné a nezbytné ochrany dat
- vypracování posouzení vlivu na ochranu osobních údajů, v angličtině DPIA neboli Data Protection Impact Assessment
- jmenování pověřence pro ochranu osobních údajů neboli DPO (Data Protection Officer)
- zavedení tzv. pseudonymizace osobních údajů
- vedení záznamů o činnostech zpracování
- konzultace s dozorovým orgánem před samotným zpracováním osobních údajů

Dalším principem spadajícím do oblasti zodpovědnosti je povinnost správců nebo zpracovatelů vést záznamy o činnostech zpracování, za které zodpovídají. Každý správce a zpracovatel bude povinen spolupracovat s dozorovým úřadem a na jeho žádost mu tyto záznamy zpřístupnit, aby na jejich základě mohly být tyto operace zpracování monitorovány.
Tyto záznamy o činnostech musí obsahovat následující informace:

- jméno a kontaktní údaje správce a zpracovatele včetně jména DPO
- účely zpracování
- popis kategorií subjektů údajů a kategorií osobních údajů
- kategorie příjemců, kterým byly nebo budou údaje zpřístupněny
- informace o mezinárodním předávání osobních údajů
- lhůty pro výmaz jednotlivých kategorií údajů
- popis technických a organizačních opatření

Výjimky z povinnosti vést záznamy o činnostech zpracování lze uplatnit pro organizaci s méně než 250 zaměstnanci, pokud zpracování osobních údajů není jejich hlavní činností, neexistuje u nich riziko pro práva a svobody osob a tyto organizace nezpracovávají citlivé údaje.

## DATA PROTECTION OFFICER (DPO)

Důležitým pilířem prokazování souladu s GDPR je jmenování tzv. pověřence pro ochranu osobních údajů neboli DPO (anglicky Data Protection Officer).

Hlavním úkolem DPO je monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z nařízení, provádění interních auditů, školení pracovníků a celkové řízení agendy interní ochrany dat.

Povinnost pověřence jmenovat nastává ve třech případech, pokud:

1. zpracování provádí orgán veřejné moci či veřejný subjekt (s výjimkou soudů),
2. hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování občanů,
3. hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Ve všech třech případech by měla být správci nebo zpracovateli nápomocna osoba s odbornými znalostmi v oblasti právních předpisů a postupů týkajících se ochrany údajů. Tito pověřenci, bez ohledu na to, zda se jedná o zaměstnance správce, nebo externě poskytovanou službu, by měli být schopni plnit své povinnosti a úkoly nezávislým způsobem. Některé organizace mohou dospět k závěru, že dobrovolné jmenování pověřence může být užitečné, což budou dozorové orgány podporovat.

Podle nařízení může být jediný pověřenec jmenován i pro několik státních orgánů, institucí či firem, které mají podobnou organizační strukturu. V odpovědnosti pověřence jsou rozmanité úkoly, proto musí správce zajistit, aby je jediný pověřenec zvládl plnit efektivně i přesto, že má odpovědnost za několik orgánů veřejné moci nebo veřejných subjektů. Osobní dostupnost pověřence (fyzická ve stejných prostorách jako zaměstnanci, po horké lince nebo jiným zabezpečeným komunikačním prostředkem) je nezbytná, aby měl občan jistotu, že ho dokáže kontaktovat. Pověřenec je při výkonu svých úkolů vázán tajemstvím nebo důvěrností v souladu s právem Unie nebo členských států.
Příklady rozsáhlého zpracování osobních údajů:

- zpracování údajů o pacientech v rámci běžné činnosti nemocnice
- zpracování cestovních dat jednotlivců používajících městskou hromadnou dopravu (např. sledování prostřednictvím čipové průkazky)
- zpracování údajů o aktuální zeměpisné poloze zákazníků
- zpracování zákaznických dat v rámci běžné obchodní činnosti pojišťovny nebo banky
- zpracování osobních údajů vyhledávačem pro potřeby behaviorální reklamy
- zpracování obsahových, provozních či lokalizačních dat poskytovatelem telefonních a internetových služeb

Příklady zpracování, která nejsou rozsáhlá:

- zpracování údajů o pacientech jednotlivým lékařem
- zpracování osobních údajů týkající se rozsudků v trestních věcech a trestných činů jednotlivým právníkem

Pravidelné a systematické monitorování jasně zahrnuje všechny formy sledování a profilování na internetu, i pro účely behaviorální reklamy. Uveďme opět pár příkladů:

- provozování telekomunikační sítě nebo telekomunikačních služeb
- cílení internetové reklamy pomocí e-mailu
- profilování a bodování (skórování) pro účely posouzení rizik (např. pro účely hodnocení úvěrového rizika, stanovení výše pojistného, předcházení podvodům, odhalování praní peněz)
- sledování polohy, například u mobilních aplikací
- věrnostní programy
- behaviorální reklama; sledování zdravého životního stylu, tělesné kondice a zdravotních dat pomocí na těle nositelných zařízení
- kamerové systémy

Pověřenci nenesou osobní odpovědnost za nedodržování GDPR. Nařízení jasně stanoví, že jsou to správci nebo zpracovatelé, kteří musí zajistit a být schopni doložit, že zpracování je prováděno v souladu s GDPR. Právní soulad v oblasti ochrany dat je odpovědností správce nebo zpracovatele.

## SANKCE SPRÁVCŮ DAT

V případě porušení, nezavedení či nepřipravenosti na nové nařízení hrozí povinným subjektům vysoké pokuty, které mohou být v mnoha případech až likvidační.

GDPR po vzoru předpisů na ochranu hospodářské soutěže zavádí několikanásobně vyšší pokuty, než jsme byli doposud zvyklí. Jejich maximální výše je 20.000.000 eur nebo 4 % z celkového ročního obratu společnosti (vyšší z obou možností) a bude záviset na řadě faktorů, jako je např. povaha, závažnost a délka porušování, počet poškozených občanů a míra škody, kroky podniknuté správcem či zpracovatelem ke zmírnění škod, kategorie osobních údajů dotčené porušením a řada dalších.

Je důležité zdůraznit, že maximální výše pokuty může být udělena jak menší společnosti s pěti zaměstnanci, tak velké nadnárodní korporaci, pokud neučiní kroky nezbytné k uvedení do souladu s principy a povinnostmi vyplývajícími z GDPR.

Kromě udělení těchto správních pokut mohou být správci či zpracovatelé osobních údajů navíc vystaveni žalobám podaným fyzickými osobami s nárokem na náhradu škody v případě hmotné či nehmotné újmy. V neposlední řadě jsou společnosti vystaveny ztrátě důvěry a reputačním rizikům způsobeným nesprávným zacházením s osobními údaji.

**Adresa:** Společnost
Podané ruce o.p.s.
Hilleho 5, 602 00 Brno

**T:** +420 545 247 535
**M:** +420 777 916 285
**E:** info@podaneruce.cz

**Bankovní spojení:** Oberbank AG 2231107576/8040
**DIČ:** CZ60557621
**IČO:** 60557621