



**(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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), GDPR – General Data Protection Regulation)**

Dne **25. 5. 2018** nabylo účinnosti nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „nařízení“), které k datu nabytí účinnosti nahradilo zákon č. 101/2000 Sb., o ochraně osobních údajů. Tuto evropskou právní úpravu pak doplňuje zákon č. 110/2019 Sb., o zpracování osobních údajů, který nabyl účinnosti dne 24. dubna 2019.

Nová právní úprava neznamená zásadní předěl v přístupu k ochraně osobních údajů, pouze se nad rámec dosavadní praxe stanoví několikero nových povinností pro správce a zpracovatele a práv subjektů, jejichž osobní údaje se zpracovávají. Základní principy spojené s nakládáním s osobními údaji, kterými se ochrana osobních údajů dosud řídila, se nikterak nemění. Lze tedy shrnout, že pokud byly osobní údaje zpracovávány v souladu se zákonem o ochraně osobních údajů, pak nebude nutné příliš do zavedených postupů zasahovat. V této souvislosti je nutné si nicméně uvědomit, že osobním údajem je nejen jméno a příjmení konkrétní osoby, příp. jakýkoliv jiný údaj, který umožní konkrétní osobu ztotožnit (tedy i telefonní číslo, emailová adresa, bydliště atp.), ale i další údaje, které se konkrétní osoby týkají, které by Správce osobních údajů shromažďoval v souvislosti s takto identifikovaným subjektem údajů.

Z novinek obsažených v nové právní úpravě lze uvést povinnost správce vést záznamy o činnostech zpracování, povinnost jmenovat pověřence pro ochranu osobních údajů (tam, kde to GDPR nařizuje), zpřísnění provozu kamerových systémů a nutnosti zpracování balančních testů pro jejich provoz. Pokud jsou při zpracování rozsáhlým způsobem ohrožena práva a svobody fyzických osob, musí správce vypracovat posudek vlivu na ochranu osobních údajů, (angličtině Data Protection Impact Assessment – DPIA), případně by měl zpracovat posouzení, proč DPIA není nutno zpracovávat.

## Zásady zpracování osobních údajů-článek 5 GDPR

### 1. Osobní údaje musí být:

- a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“);
- b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely („účelové omezení“);
- c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“);
- d) přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („přesnost“);
- e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);
- f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost“);

2. Správce odpovídá za dodržení odstavce 1 a musí být schopen toto dodržení souladu doložit („odpovědnost“).

## Zákonnost zpracování-článek 6 GDPR

1. Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

- a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
- b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
- c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
- d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
- e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
- f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

## Důvody zpracování osobních údajů v praxi

### GDPR

- GDPR Článek 6 odstavec 1 písmeno a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
- GDPR Článek 6 odstavec 1 písmeno b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
- GDPR Článek 6 odstavec 1 písmeno c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
- GDPR Článek 6 odstavec 1 písmeno f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

## Zákony a vyhlášky ČR

- Zákon č. 563/1991 Sb. - Zákon o účetnictví
- Zákon č. 221/2015 Sb., kterým se mění zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a některé další zákony – Sbírka zákonů ročník 2015, částka 92, ze dne 10. 9. 2015.
- Zákon č. 262/2006 Sb. - Zákoník práce
- Zákon č. 513/1991 Sb. - Obchodní zákoník
- Zákon č. 499/2004 Sb. - Zákon o archivnictví a spisové službě a o změně některých zákonů
- Zákon č. 187/2006 Sb. - o nemocenském pojištění, v platném znění (§ 97 zákona)
- Zákon č. 582/1991 Sb. - o organizaci a provádění sociálního zabezpečení
- Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů
- Zákon č. 95/2004 Sb., o podmínkách získávání a uznávání odborné způsobilosti a specializované způsobilosti k výkonu zdravotnického povolání lékaře, zubního lékaře a farmaceuta, ve znění pozdějších předpisů;
- Vyhláška č. 185/2009 Sb., o oborech specializačního vzdělávání lékařů, zubních lékařů a farmaceutů a oborech certifikovaných kurzů, ve znění pozdějších předpisů;
- Zákon č. 96/2004 Sb., o podmínkách získávání a uznávání způsobilosti k výkonu nelékařských zdravotnických povolání a k výkonu činností souvisejících s poskytováním zdravotní péče a o změně některých souvisejících zákonů (zákon o nelékařských zdravotnických povoláních), ve znění pozdějších předpisů;
- Vyhláška č. 92/2012 Sb., o požadavcích na minimální technické a věcné vybavení zdravotnických zařízení a kontaktních pracovišť domácí péče, ve znění pozdějších předpisů;
- Vyhláška č. 99/2012 Sb., o požadavcích na minimální personální zabezpečení zdravotních služeb, ve znění pozdějších předpisů;
- Vyhláška č. 55/2011 Sb., o činnostech zdravotnických pracovníků a jiných odborných pracovníků, ve znění pozdějších předpisů

## Podmínky vyjádření souhlasu

### článek 7 GDPR

1. Pokud je zpracování založeno na souhlasu, musí být správce schopen doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů.
2. Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. Jakákoli část tohoto prohlášení, která představuje porušení tohoto nařízení, není závazná.
3. Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně snadné jako jej poskytnout.
4. Při posuzování toho, zda je souhlas svobodný, musí být důsledně zohledněna skutečnost, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné.

## Souhlas dítěte v souvislosti se službami informační společnosti

### článek 8 GDPR

1. Pokud se použije čl. 6 odst. 1 písm. a) v souvislosti s nabídkou služeb informační společnosti přímo dítěti, je zpracování osobních údajů dítěte zákonné, je-li dítě ve věku nejméně 16 let. Je-li dítě mladší 16 let, je takové zpracování zákonné pouze tehdy a do té míry, pokud byl tento souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti. Členské státy mohou pro uvedené účely právním předpisem stanovit nižší věk, ne však nižší než 13 let.

2. Správce vyvine přiměřené úsilí s ohledem na dostupnou technologii, aby v takovýchto případech ověřil, že byl souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti.
3. Odstavcem 1 není dotčeno obecné smluvní právo členských států, například pravidla týkající se platnosti, uzavírání nebo účinků smlouvy vzhledem k dítěti.

## Vaše práva podle GDPR.

Ve vztahu k Vaším osobním údajům máte zejména následující práva:

1. Právo na informace
2. Právo na přístup k osobním údajům
3. Právo nepřesné osobní údaje opravit či doplnit;
4. Právo na výmaz osobních údajů (právo být „zapomenut“) v určitých případech;
5. Právo na omezení zpracování
6. Právo na oznámení opravy, výmazu či omezení zpracování
7. Právo požadovat přenesení údajů;
8. Právo vznést námitku či stížnost proti zpracování v určitých případech;
9. Svůj souhlas se zpracováním osobních údajů kdykoli odvolat;
10. Právo být informován o porušení zabezpečení osobních údajů v určitých případech;
11. Další práva stanovená v zákoně o ochraně osobních údajů a v GDPR po nabytí jeho účinnosti.

## Definice pojmů.

**Pro účely nařízení GDPR se rozumí:**

- 1) „osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;
- 2) „zpracováním“ jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;
- 3) „omezením zpracování“ označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;
- 4) „profilováním“ jakákoliv forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu;
- 5) „pseudonymizací“ zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;
- 6) „evidencí“ jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;
- 7) „správce“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;
- 8) „zpracovatelem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;
- 9) „příjemcem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci

## To nejdůležitější z GDPR

zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování;

10) „třetí stranou“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jenž je oprávněna ke zpracování osobních údajů;

11) „souhlasem“ subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

12) „porušením zabezpečení osobních údajů“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

13) „genetickými údaji“ osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby;

14) „biometrickými údaji“ osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;

15) „údaji o zdravotním stavu“ osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;

16) „hlavní provozovnou“:

a) v případě správce s provozovny ve více než jednom členském státě místo, kde se nachází jeho ústřední správa v Unii, ledaže jsou rozhodnutí o účelech a prostředcích zpracování osobních údajů přijímána v jiné provozovně správce v Unii a tato jiná provozovna má pravomoc vymáhat provádění těchto rozhodnutí, přičemž v takovém případě je za hlavní provozovnu považována provozovna, která tato rozhodnutí přijala;

b) v případě zpracovatele s provozovny ve více než jednom členském státě místo, kde se nachází jeho ústřední správa v Unii, nebo pokud zpracovatel nemá v Unii žádnou ústřední správu, pak ta provozovna zpracovatele v Unii, kde probíhají hlavní činnosti zpracování v souvislosti s činnostmi provozovny zpracovatele, v rozsahu, v jakém se na zpracovatele vztahují specifické povinnosti podle tohoto nařízení;

17) „zástupcem“ jakákoli fyzická nebo právnická osoba usazená v Unii, která je správcem nebo zpracovatelem určena písemně podle článku 27 k tomu, aby správce nebo zpracovatele zastupovala, pokud jde o příslušné povinnosti správce nebo zpracovatele ve smyslu tohoto nařízení;

18) „podnikem“ jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost;

19) „skupinou podniků“ skupina zahrnující řídicí podnik a jím řízené podniky;

20) „závaznými podnikovými pravidly“ koncepce ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel usazený na území členského státu při jednorázových nebo souborných předáních osobních údajů správci nebo zpracovateli v jedné nebo více třetích zemích v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost;

21) „dozorovým úřadem“ nezávislý orgán veřejné moci zřízený členským státem podle článku 51;

22) „dotčeným dozorovým úřadem“ dozorový úřad, kterého se zpracování osobních údajů dotýká, neboť:

a) správce či zpracovatel je usazen na území členského státu tohoto dozorového úřadu;

b) subjekty údajů s bydlištěm v členském státě tohoto dozorového úřadu jsou nebo pravděpodobně budou zpracováním podstatně dotčeny, nebo

c) u něj byla podána stížnost;

23) „přeshraničním zpracováním“ buď:

a) zpracování osobních údajů, které probíhá v souvislosti s činnostmi provozoven ve více než jednom členském státě správce či zpracovatele v Unii, je-li tento správce či zpracovatel usazen ve více než jednom členském státě; nebo

b) zpracování osobních údajů, které probíhá v souvislosti s činnostmi jediné provozovny správce či zpracovatele v Unii, ale kterým jsou nebo pravděpodobně budou podstatně dotčeny subjekty údajů ve více než jednom členském státě;

24) „relevantní a odůvodněnou námitkou“ námitka vůči návrhu rozhodnutí za účelem posouzení, zda došlo k porušení tohoto nařízení, nebo zda je zamýšlený úkon v souvislosti se správcem či zpracovatelem v souladu s tímto nařízením, která jasně dokazuje významnost rizik vyplývajících z návrhu rozhodnutí, pokud jde o základní práva a svobody subjektů údajů, případně volný pohyb osobních údajů v rámci Unie;

25) „službou informační společnosti“ služba ve smyslu čl. 1 odst. 1 písm. b) směrnice (EU) 2015/1535 (19);

26) „mezinárodní organizací“ organizace a jí podřízené subjekty podléhající mezinárodnímu právu veřejnému nebo jiný subjekt zřízený dohodou mezi dvěma nebo více zeměmi nebo na jejím základě.

## Hlavní zásady pro ochranu osobních údajů.

### 1. Hlavní povinnosti Správce osobních údajů, jeho zaměstnanců, případně dalších osob při nakládání s osobními údaji.

1.1 Každý zaměstnanec Správce osobních údajů je povinen počínat si tak, aby neohrozil ochranu osobních údajů zpracovávaných Správcem osobních údajů.

1.2 Dále je každý zaměstnanec Správce osobních údajů povinen

- zamezit nahodilému a neoprávněnému přístupu k osobním údajům zaměstnanců a dalších osob, které Správec zpracovává,
- pokud zjistí porušení ochrany osobních údajů, neoprávněné použití osobních údajů, zneužití osobních nebo jiné neoprávněné jednání související s ochranou osobních údajů, bezodkladně zabránit dalšímu neoprávněnému nakládání, zejména zajistit znepřístupnění, a ohlásit tuto skutečnost statutárnímu orgánu nebo pověřené osobě Správce osobních údajů či jinému příslušnému zaměstnanci.

1.3 Statutární orgán Správce osobních údajů je povinen

- informovat zaměstnance o všech významných skutečnostech, postupech nebo událostech souvisejících s nakládáním s osobními údaji, a to bez zbytečného odkladu,
- zajistit, aby zaměstnanci Správce byli řádně poučeni o právech a povinnostech při ochraně osobních údajů,
- zajišťovat, aby zaměstnanci Správce byli podle možností a potřeb Správce osobních údajů vzdělávání nebo proškolení o ochraně osobních údajů

### 2. Při nakládání s osobními údaji se Správec, jeho zaměstnanci a další osoby řídí těmito zásadami:

- Postupovat při nakládání s osobními údaji v souladu s právními předpisy,
- S osobními údaji nakládat uvážlivě, souhlas se zpracováním osobních údajů nenadužívat,
- Zpracovávat osobní údaje ke stanovenému účelu a ve stanoveném rozsahu a dbát na to, aby tyto byly pravdivé a přesné,
- Zpracovávat osobní údaje v souladu se zásadou zákonnosti – na základě právních předpisů, při plnění ze smlouvy, při plnění právní povinnosti správce, při ochraně životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (zejména děti požívají vyšší ochrany), při ochraně oprávněných zájmů Správce osobních údajů, při ochraně veřejného zájmu, a zpracování osobních údajů na základě souhlasu,
- Respektovat práva člověka, který je subjektem údajů, zejména práva dát a odvolat souhlas se zpracováním, práva na výmaz, namítat rozsah zpracování apod.,
- Poskytovat při zpracování osobních údajů zvláštní ochranu dětem,
- Poskytovat informace o zpracování osobních údajů, komunikovat,
- Při uzavírání smluv a právním jednání postupovat se zřetelem na povinnost chránit osobní údaje před zneužitím,
- Spolupracovat s pověřencem pro ochranu osobních údajů.

### 3. Postupy Správce osobních údajů, jeho zaměstnanců, případně dalších osob při nakládání s osobními údaji

3.1 Správce všechny osobní údaje, se kterými nakládá a které zpracovává, chrání vhodnými a dostupnými prostředky před zneužitím. Přitom Správce především uchovává osobní údaje v prostorách, na místech, v prostředí nebo v systému, do kterého má přístup omezený, předem stanovený a v každý okamžik alespoň statutárnímu orgánu nebo pověřené osobě Správce osobních údajů známý okruh osob; jiné osoby mohou získat přístup k osobním údajům pouze se svolením statutárního orgánu Správce osobních údajů nebo jím pověřené osoby.

3.2 Správce zavede taková opatření, aby o nakládání a zpracování osobních údajů měl přehled alespoň statutární orgán osobních údajů nebo jím pověřená osoba a pověřenec pro ochranu osobních údajů. **Mezi tato opatření patří např. ústní nebo písemná informace, písemná komunikace, stanovení povinností v pracovní smlouvě, v dohodě o provedení práce, v dohodě o pracovní činnosti, ve smlouvě, kterou Správce uzavírá se třetí osobou (nájemní smlouva, smlouva o dílo, smlouva o poskytování služeb).**

3.3 Správce alespoň jednou za rok provede zhodnocení postupů při nakládání a zpracování osobních údajů. Zhodnocení může být provedeno dle zvyklostí Správce osobních údajů, zpravidla se učiní stručný záznam např. v zápisu z porady. Zjistí-li se, že některé postupy Správce osobních údajů jsou zastaralé, zbytečné nebo se neosvědčily, učiní Správce bezodkladně nápravu.

3.4 Každý zaměstnanec Správce osobních údajů při nakládání s osobními údaji respektuje jejich povahu, tedy že jde o součást soukromí člověka jako subjektu údajů, a tomu přizpůsobí úkony s tím spojené. Zaměstnanec zejména osobní údaje nezveřejňuje bez ověření, že takový postup je možný, nezpřístupňuje osobní údaje osobám, které neprokážou právo s nimi nakládat. Zaměstnanec, vyplývá-li taková povinnost z jiných dokumentů, informuje subjekt údajů o jeho právech na ochranu osobních údajů; jinak odkáže na statutární orgán Správce osobních údajů nebo jím určenou osobu nebo na pověřence pro ochranu osobních údajů.

3.5 Správce při nakládání a zpracování osobních údajů aktivně spolupracuje s pověřencem pro ochranu osobních údajů.

3.6 Správce ihned řeší každý bezpečnostní incident týkající se osobních údajů, a to i v součinnosti s pověřencem pro ochranu osobních údajů. V případě, že je pravděpodobné, že incident bude mít za následek vysoké riziko pro práva a svobody fyzických osob, především konkrétního zaměstnance, Správce tuto osobu vždy informuje a sdělí, jaká opatření k nápravě přijala. O každém incidentu se sepiše záznam. O každém závažném incidentu Správce informuje Úřad pro ochranu osobních údajů.

3.7 Vzhledem k tomu, že Správce eviduje v podstatě údaje o zaměstnancích, které stanovují právní předpisy (zejména Zákoník práce a pracovněprávní předpisy), nemá oznamovací povinnost vůči Úřadu pro ochranu osobních údajů.

3.8 Organizační opatření k ochraně osobních údajů

3.8.1 Materiály, které obsahují osobní údaje zaměstnanců, jsou trvale uloženy v uzamykatelných skříních.

3.8.2 Při práci s elektronickou evidencí nesmí oprávněné osoby opouštět počítač bez odhlášení se, nemohou nechat nahlížet žádnou jinou osobu a musí chránit utajení přihlašovacím hesla; a v případě nebezpečí jeho vyjádření jej ihned (ve spolupráci se správcem sítě) změnit. Přístupy nastavuje pověřený zaměstnanec Správce osobních údajů – správce počítačové sítě, který nastavuje potřebné zabezpečení dat a počítačové sítě (dle pokynů Správce).

3.8.3 Osobní spisy zaměstnanců jsou uloženy v uzamykatelných skříních přístup k nim má statutární orgán Správce osobních údajů, jím pověřené osoby a osoby u nichž pověření pramení z pracovního zařazení.

3.8.4 Zaměstnanci mají právo seznámit se s obsahem svého osobního spisu. O tomto právu jsou zaměstnanci poučeni, zpravidla při uzavření pracovního poměru.

3.8.5 Zaměstnanci Správce neposkytují bez právního důvodu žádnou formou osobní údaje jiných zaměstnanců cizím osobám a institucím, tedy ani telefonicky ani mailem ani při osobním jednání.

3.8.6 Písemná hodnocení a posudky, která se odesílají mimo firmu nebo organizaci, např. pro potřeby soudního řízení, přijímacího řízení, zpracovávají zaměstnanci určení statutárním zástupcem Správce. Nejsou však oprávněni samostatně tato hodnocení podepisovat, poskytovat a odesílat jménem Správce osobních údajů a mají povinnost zachovávat mlčenlivost o dané věci.

## To nejdůležitější z GDPR

3.8.7 Seznamy zaměstnanců se nezveřejňují, neposkytují bez vědomého souhlasu zaměstnanců jiným fyzickým či právnickým osobám nebo orgánům, které neplní funkci orgánu nadřízeného firmě či organizaci nebo nevyplývá-li to ze zákona.

3.8.8 V propagačních materiálech Správce osobních údajů, ve výroční zprávě či ročence Správce osobních údajů, na firemním webu apod. lze s obecným souhlasem zaměstnanců uveřejňovat výhradně textové či obrazové informace o firemních akcích. Při publikování v tisku se autor dotazuje na souhlas příslušného zaměstnance. Zaměstnanec má právo požadovat bezodkladné zablokování či odstranění informace či fotografie či záznamu týkající se jeho osoby, který zveřejňovat nechce.

3.8.9 Psychologické, lékařské a jiné průzkumy a testování mezi zaměstnanci, jejichž součástí by bylo uvedení osobních údajů zaměstnance, lze provádět jen se souhlasem.

3.8.10 Pokud jsou pro vedení dokumentace využívány formuláře a software, je nutné provést kontrolu, zda nepožadují či nenabízejí evidenci nadbytečných údajů a tyto údaje nezpracovávat.

3.8.11 Ve firmě nebo organizaci se neprovozují kamerové systémy sledující prostory používané zaměstnanci Správce osobních údajů v dob jinak než ze zákonných důvodů – viz. GDPR článek 6 odstavec 1 písmeno (f).

3.8.12 Uzavírá-li Správce jakoukoli smlouvu (nájemní smlouvu, smlouvu o dílo, smlouvu o poskytnutí služeb, nepojmenovanou smlouvu apod.), k jejímuž plnění je zapotřebí druhé smluvní straně poskytnout osobní údaje, Správce vždy a bezpodmínečně bude trvat na tom, aby ve smlouvě byla druhé smluvní straně uložena povinnost:

- přijmout všechna bezpečnostní, technická, organizační a jiná opatření s přihlédnutím ke stavu techniky, povaze zpracování, rozsahu zpracování, kontextu zpracování a účelům zpracování k zabránění jakéhokoli narušení poskytnutých osobních údajů,
- nezapojit do zpracování žádné další osoby bez předchozího písemného souhlasu Správce osobních údajů,
- zpracovávat osobní údaje pouze pro plnění smlouvy (vč. předání údajů do třetích zemí a mezinárodních organizací); výjimkou jsou pouze případy, kdy jsou určité povinnosti uloženy přímo právním předpisem,
- zajistit, aby se osoby oprávněné zpracovávat osobní údaje u dodavatele byly zavázány k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,
- zajistit, že dodavatel bude Správci bez zbytečného odkladu nápomocen při plnění povinností Správce osobních údajů, zejména povinnosti reagovat na žádosti o výkon práv subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 nařízení, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 nařízení, povinnosti posoudit vliv na ochranu osobních údajů dle čl. 35 nařízení a povinnosti provádět předchozí konzultace dle čl. 36 nařízení, a že za tímto účelem zajistí nebo přijme vhodná technická a organizační opatření, o kterých ihned informuje Správce,
- po ukončení smlouvy řádně naložit se zpracovávanými osobními údaji, např. že všechny osobní údaje vymaže, nebo je vrátí Správci a vymaže existující kopie apod.,
- poskytnout Správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené Správci právními předpisy,
- umožnit kontrolu, audit či inspekci prováděné Správce osobních údajů nebo příslušným orgánem dle právních předpisů,
- poskytnout bez zbytečného odkladu nebo ve lhůtě, kterou stanoví Správce, součinnost potřebnou pro plnění zákonných povinností Správce osobních údajů spojených s ochranou osobních údajů, jejich zpracováním,
- poskytnuté osobní údaje chránit v souladu s právními předpisy,
- přiměřeně postupovat podle této směrnice, která je přílohou smlouvy.

## 4. Pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchovávání osobních údajů.

4.1 Správce nakládá a zpracovává pouze osobní údaje, které



## To nejdůležitější z GDPR

- souvisejí s pracovním a mzdovým zařazením zaměstnanců či smluvních pracovníků, se sociálním, a zdravotním pojištěním (např. dosažené vzdělání, délka praxe, funkční zařazení apod.),
- souvisejí s jednoznačnou identifikací zákonných zástupců zaměstnanců v souladu se zákonem (jméno, příjmení, bydliště, kontakt, např. telefonní číslo pro případ nutného kontaktu Správce osobních údajů s rodinným příslušníkem v rámci ochrany zdraví, bezpečnosti a práv zaměstnance, další údaje nezbytné např. pro vydání správního rozhodnutí apod.
- souvisejí s identifikací zaměstnance ze zákona (datum narození, místo narození, rodné číslo, státní příslušnost, bydliště, nutný zdravotní údaj apod.
- jsou nezbytné pro plnění právní povinnosti, ochranu oprávněných zájmů Správce osobních údajů nebo ve veřejném zájmu,
- k jejichž zpracování získal Správce souhlas subjektu údajů.

4.2 Osobní údaje se uchovávají pouze po dobu, která je nezbytná k dosažení účelu jejich zpracování, včetně archivace.

4.3 K osobním údajům mají přístup osoby k tomu oprávněné zákonem nebo na základě zákona.

Do jednotlivých dokumentů Správce osobních údajů, které obsahují osobní údaje, mohou nahlížet

- do osobního spisu zaměstnance vedoucí zaměstnanci, kteří jsou zaměstnanci nadřízení. Právo nahlížet do osobního spisu má orgán inspekce práce, úřad práce, soud, státní zástupce, příslušný orgán Policie České republiky, Národní bezpečnostní úřad a zpravodajské služby. Zaměstnanec má právo nahlížet do svého osobního spisu, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených, a to na náklady zaměstnavatele (§ 312 zákoníku práce),
- do spisu, vedeném ve správním řízení účastníci správního řízení, vedoucí pracovníci Správce nebo osoba, která je zmocněna s úředním spisem pracovat po dobu řízení.

## Závěr.

Pokud ještě v této publikaci nenašli odpověď na Vaši otázku, kontaktujte naši bezplatnou poradnu na www stránkách <https://www.everyregard.one> nebo volejte **+420 607 888 494**.

**Miroslav Kalinský**

GDPR konzultant

**EVERY REGARD s.r.o.**  
Žamosstří 1155/27  
Ostrava, Slezská Ostrava, 710 00  
IČO: 05460034, společnost není plátcem DPH

V Ostravě dne 2.2.2021