|  |
| --- |
| Název dokumentu:Interní směrnice pro zajištění ochrany osobních údajů v SPZ DESIGN, s.r.o. |
| Účel a obsah dokumentu:Promítnutí požadavků obecně závazných právních předpisů do systému jakosti ČMI**Implementace zákona o ochraně osobních údajů a nařízení GDPR**  |
| Závaznost pro: **všechny zaměstnance firmy** |
| Nahrazuje a/nebo souvisí s dokumentem:první vydání s účinností od: 25.5.2018 |
| Zpracoval: Ing. Petr Zavadil | Přezkoumal:Ing. Petr Zavadil  | Schválil a vydal:Ing. Petr Zavadil  |

**Schváleno: 25.5.2018**

**Vydáno: 25.5.2018**

**Účinnost: 25.5.2018 do odvolání**

# **Obsah dokumentu**

1. Obsah dokumentu 2

2. Platnost a historie změn 3

2.1. Změny 3

3. Preambule 4

4. Úvodní ustanovení 5

4.1. Základní pojmy 5

4.2. Osobní údaje zpracovávané organizací 6

**4.2.1.** Osobní údaje uchazečů o zaměstnání 6

**4.2.2.** Osobní údaje zaměstnanců 6

**4.2.3.** Osobní údaje zaměstnanců po skončení pracovního poměru 7

**4.2.4.** Osobní údaje dalších subjektů smluvních vztahů organizace 7

**4.2.5.** Záznamy o činnostech zpracování osobních údajů 8

4.3. Zabezpečení osobních údajů 9

**4.3.1.** Oprávnění zaměstnanců 9

**4.3.2.** Organizační opatření 9

**4.3.3.** Technická opatření 9

4.4. Povinnosti zaměstnanců při zpracování osobních údajů 9

4.5. Práva subjektu údajů 11

**4.5.1.** Právní základ pro zpracování 11

**4.5.2.** Právo na informace 11

**4.5.3.** Právo na přístup 11

**4.5.4.** Právo na výmaz 11

**4.5.5.** Zjištění totožnosti subjektu údajů 12

**4.5.6.** Informační povinnost vůči zaměstnancům 12

4.6. Zpracování osobních údajů zpracovatelem 12

4.7. Postup organizace a zaměstnanců při porušení zabezpečení osobních údajů 12

**4.7.1.** Hlášení událostí s vlivem na ochranu osobních údajů 13

**4.7.2.** Způsob zvládání událostí 13

**4.7.3.** Způsob hlášení incidentů 13

**4.7.4.** Oznamování incidentů subjektům údajů 13

5. Závěrečná ustanovení 14

# Platnost a historie změn

Dokument byl vydán jako součást dokumentace GDPR a připomínkován v následujících verzích:

## Změny

|  |  |  |  |
| --- | --- | --- | --- |
| Verze | Změna: | Datum: | Popis: |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Preambule

Organizace je podle zákona č. 101/2000 Sb., o ochraně osobních údajů (dále jen Zákon), ve znění pozdějších předpisů, správcem osobních údajů. V souvislosti s přijetím nové právní úpravy ochrany osobních údajů na úrovni EU obsažené v Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 (dále jen „GDPR“), účinného od **25. 05. 2018**, je nezbytné provést v rámci organizace úpravu vnitřních organizačních pravidel a postupů týkající se ochrany a zpracování osobních údajů, která stanoví závazné podmínky pro zpracování osobních údajů zaměstnanci organizace při výkonu jejich činnosti s cílem zabezpečit v co možná největší míře možnému úniku, zneužití či jinému porušení ochrany těchto údajů.

Pro stanovení základních podmínek ochrany osobních údajů při zpracovávání osobních údajů v organizaci a splnění dalších náležitostí vyžadovaných Zákonem, recitálem 78 GDPR a souvisejícími ustanoveními závaznými pro správce, vydávám:

**Interní směrnici pro zajištění ochrany osobních údajů**

, dále také jako „**interní směrnice**“ nebo „**směrnice**“ nebo „**zásady**“.

Tato směrnice má charakter vnitřní koncepce ve smyslu recitálu 78 GDPR.

# Úvodní ustanovení

## Základní pojmy

**osobní údaje** – veškeré informace o identifikované nebo identifikovatelné fyzické osobě (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;

**zvláštní kategorie osobních údajů** – osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby;

**zpracování osobních údajů** – jakákoliv operace nebo soubor operací s osobními údaji, která je prováděna 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;

**pseudonymizace** – 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;

**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;

**příjemce** – 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.

**souhlas 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;

**zpracovatel** – je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;

**evidence** – jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;

**výmaz osobních údajů** – fyzické zničení nosičů, jejich fyzické vymazání nebo trvalé vyloučení z dalších zpracování;

**omezení zpracování osobních údajů –** označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;

**porušení 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;

**dozorový úřad –** nezávislý orgán zřízený členským státem EU, který je pověřen monitorováním uplatňování požadavků na ochranu osobních údajů; v ČR je tímto orgánem Úřad pro ochranu osobních údajů.

## Osobní údaje zpracovávané organizací

### Osobní údaje uchazečů o zaměstnání

Osobní údaje získané od uchazečů o zaměstnání (životopisy, motivační dopisy, doklady o kvalifikaci atd.) poskytnuté v rámci výběrového řízení mohou být zpracovávány pouze pro účely a v rozsahu nezbytném pro provedení a vyhodnocení uchazečů v rámci tohoto výběrového řízení. Oprávnění zpracovávat tyto údaje náleží zaměstnancům personalistiky, kteří realizují předmětné výběrové řízení a posuzují vhodnost jednotlivých uchazečů.

Po ukončení výběrového řízení jsou zaměstnanci provádějící výběrové řízení povinni provést výmaz všech poskytnutých osobních údajů a dokladů od uchazečů v listinné i elektronické podobě, s výjimkou situace, kdy uchazeč poskytl výslovný souhlas se zpracováním svých osobních údajů i pro případná další výběrová řízení, která bude organizace realizovat v budoucnu.

Vedoucí zaměstnanci, popř. určení zaměstnanci jsou povinni informovat případné uchazeče o výše uvedených zásadách zpracování osobních údajů v textu inzerátu, kterým je výběrové řízení zveřejněno.

### Osobní údaje zaměstnanců

Osobní údaje zaměstnanců organizace, zejména adresní a identifikační údaje, jsou zpracovávány pro účely pracovněprávní, důchodového zabezpečení, nemocenského pojištění, zdravotního pojištění a daně ze závislé činnosti, a to v rozsahu nezbytném pro splnění zákonných povinností organizace jako zaměstnavatele.

Výkon činností zahrnujících zpracování osobních údajů zaměstnanců pro účely pracovněprávní, důchodového zabezpečení, nemocenského pojištění a zdravotního pojištění je v působnosti Ing. Petra Zavadila. Osobní údaje zaměstnanců jsou vedeny jak v elektronické podobě, tak v listinné podobě.

Osobní údaje jsou v elektronické podobě vedeny v interních informačních systémech – icloud. Osobní údaje jsou v těchto informačních systémech zpřístupněny určeným zaměstnancům, každý z těchto zaměstnanců má však přístup pouze k těm osobním údajům zaměstnanců, které jsou nezbytné pro plnění pracovních povinností v rámci jeho pracovní pozice a pracovní náplně.

Zaměstnavatel zpracovává následující osobní údaje:

* příjmení, jméno, datum narození, státní občanství, adresa pro doručování písemností zaměstnanci,
* rodné číslo,
* vznik a (pokud již tento stav nastal) skončení pracovněprávního vztahu,
* záznam o tom, zda občan pobírá důchod; v kladném případě číslo rozhodnutí o přiznání důchodu,
* mzdový list, evidenční list důchodového pojištění,
* podepsané daňové prohlášení,
* údaje o vyplacených náhradách za ztrátu na výdělku po skončení pracovní neschopnosti náležející za pracovní úraz nebo nemoc z povolání (pokud tento stav nastal).

Zpracování osobních údajů pro zúčtování a výplatu mzdy zajišťuje Ing. Petr Zavadil a externí účetní.

### Osobní údaje zaměstnanců po skončení pracovního poměru

Zaměstnavatel je povinen ponechat si s ohledem na plnění zákonných požadavků některé doklady (pracovní smlouvy, dohody o čerpání neplaceného volna, dohody o provedení práce, dohody o pracovní činnosti, evidenční listy, mzdové výměry atd.) po skončení pracovního poměru / DPP / DPČ pro účely důchodového zabezpečení (pojištění), nemocenského pojištění a zdravotního pojištění a případně pro plnění dalších právních povinností správce, při zajištění ochrany těchto údajů v souladu se zákonem. Doba uchování těchto dokladů je stanovena příslušnými právními předpisy.

Další doklady z osobního spisu zaměstnance (např. životopisy, ověřené kopie dokladů o vzdělání atd.) je organizace oprávněna uchovávat pro účely případného vypořádání nároků mezi zaměstnancem a organizací vyplývající z pracovní smlouvy po dobu **5 let od skončení pracovního poměru**.

Po skončení pracovního poměru / DPP / DPČ zaměstnance organizace provede blokaci e-mailové schránky zaměstnance a znepřístupnění osobních údajů. Osobní údaje **zaměstnance** budou vymazány z evidencí organizace ve lhůtě **5 let od skončení pracovního poměru**. Další zpracování osobních údajů zaměstnance se řídí výlučně zákonným právním rámcem – zejména zákonem o důchodovém zabezpečení a pod.

Zaměstnanec je povinen při skončení pracovněprávního vztahu vymazat ze všech zařízení svěřených organizací veškeré soukromé záznamy, které se nevztahují k výkonu práce u organizace zaměstnavatele. V případě, že zaměstnavatel po skončení pracovněprávního vztahu zaměstnance zjistí, že se v některém ze zařízení nachází osobní záznamy zaměstnance, má organizace právo je bez dalšího a bez náhrady vymazat.

### Osobní údaje dalších subjektů smluvních vztahů organizace

Dalším účelem zpracování osobních údajů v organizaci je jednání o smluvním vztahu a plnění smluv. V souvislosti s plněním některých z těchto předmětů činnosti organizace, dochází rovněž ke zpracování a shromažďování osobních údajů.

V **informačním systému – icloud** jsou zpracovávány osobní údaje (adresní a identifikační údaje, ekonomické a účetní údaje apod.) zákazníků, dodavatelů a popř. dalších subjektů smluvního vztahu s organizací, které jsou nezbytné pro splnění uzavřené smlouvy. Jde o datový soubor uspořádaný a přístupný jednotlivým zaměstnancům v závislosti na jejich pracovní pozici a pracovní náplni.

V **informačním systému - icloud** z důvodu oprávněného zájmu organizace pro účely řádného plnění smluv, efektivní komunikace v rámci smluvního vztahu a usnadnění vymáhání pohledávek dále zpracována osobní údaje zaměstnanců zákazníků (jméno a příjmení, pracovní e-mail, pracovní telefonní číslo), které zákazník uvedl jako kontaktní osoby ve věcech realizace předmětu těchto smluvních vztahů. Poučení o zpracování shora uvedených osobních údajů je součástí uzavíraných smluv.

Pro účely řádného plnění smluvních vztahů a usnadnění vymáhání pohledávek mohou být taktéž uváděny osobní údaje zaměstnanců subjektu smlouvy (v rozsahu jméno a příjmení, pracovní e-mail, pracovní telefonní číslo), které subjekt smlouvy uvedl jako kontaktní osoby ve věcech smlouvy. Poučení o zpracování shora uvedených osobních údajů je součástí uzavíraných smluv formou doložky.

Mimo výše uvedené případy, pokud se jedná o zpracování nad rozsah nezbytný pro plnění smlouvy, musí být zajištěn písemný souhlas se zpracováním těchto osobních údajů, a to zaměstnancem organizace, který předmětnou činnost zajišťuje. Tento písemný souhlas může být například součástí (přihlášky na školení atd.). Fyzické osoby poskytují správci souhlas se zpracováním osobních údajů svým podpisem předmětného dokumentu, jejíž součástí je i poučení dle platných právních předpisů.

Evidence souhlasů subjektů údajů – fyzických osob je vedena v informačním systému icloud a na záložním disku.

Evidence veškerých zákazníků on-line služeb organizace je vedena **v informačním systému icloud a záložním disku.**

Ke všem výše uvedeným programům, které jsou v rámci organizace používány, mají přístupová práva pouze pověření zaměstnanci organizace na základě přístupových oprávnění nastavených v systému řízení přístupu –Ing. Petr Zavadil a jím pověřená osoba (např. IT specialista). Přístup je zabezpečen heslem a práce s příslušným serverem probíhá pouze prostřednictvím šifrované komunikace.

### Záznamy o činnostech zpracování osobních údajů

Organizace vede záznamy o činnostech zpracování osobních údajů, za něž odpovídá. Záznamy o činnostech zpracování osobních údajů nahrazují oznamovací povinnost stanovenou Zákonem, přičemž na požádání musí být tyto záznamy poskytnuty Úřadu pro ochranu osobních údajů. Záznamy o činnostech zpracování musí být vyhotoveny v písemné podobě nebo elektronicky. Vytvořením a vedením tohoto záznamu je v rámci organizace pověřeno vedení organizace.

Záznamy o činnostech zpracování osobních údajů musí obsahovat následující informace:

* účely zpracování,
* popis kategorií subjektů údajů,
* kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny,
* je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů,
* je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.

## Zabezpečení osobních údajů

Firma je povinna zavést, evidovat a aktualizovat vhodná a účinná technická a organizační opatření pro zajištění ochrany osobních údajů, za něž odpovídá.

Evidence, plánování a aktualizace opatření vede organizace ve formě záznamů v informačním systému icloud.

Vytvořením a vedením tohoto záznamu je v rámci organizace pověřen zaměstnanec Ing. Petr Zavadil a jím pověřená osoba.

Procesy schvalování a rozhodování o aplikaci příslušných opatření se řídí nastaveným způsobem řízení organizace.

### Oprávnění zaměstnanců

Zaměstnanci organizace nejsou oprávněni zpracovávat osobní údaje nad rámec svých povinností stanovených těmito zásadami, záznamy o činnostech zpracování osobních údajů a pracovní náplní.

### Organizační opatření

Ochrana osobních údajů je v organizaci zajištěna určením konkrétních zaměstnanců, kteří mají přístup k osobním údajům a provádí jejich zpracování, stanovením povinností těmto zaměstnancům s ochranou osobních údajů souvisejících a kontrolou dodržování těchto povinností. Stanovení podmínek a rozsahu osobních údajů zpracovávaných určenými zaměstnanci je dáno těmito zásadami, záznamy o činnostech zpracování osobních údajů a konkrétními pracovními náplněmi zaměstnanců.

### Technická opatření

Ochrana osobních údajů z hlediska technického zabezpečení je v organizaci zajištěna technickými prostředky, jimiž jsou uzamykatelné dveře kanceláří, úschovné uzamykatelné skříně a trezory pro fyzickou bezpečnost nosičů osobních údajů (listinné dokumenty, diskety, CD-ROM, USB a Flash disky atd.). Dokumenty uchovávané v elektronické podobě jsou chráněny opatřeními zajišťujícími počítačovou bezpečnost, a to zejména šifrováním a řízením přístupu. Přístup hesly je zabezpečen také do informačních systémů a softwaru, kde jsou zpracovávány osobní údaje.

**Je zakázáno kopírovat jakékoli osobní údaje na fyzické či elektronické nosiče dat a tyto vynášet mimo zabezpečené prostory organizace. Veškeré fyzické a elektronické nosiče dat obsahující jakékoli osobní údaje, které jsou určeny pro přenos dat musí být dostatečně fyzicky či elektronicky zabezpečeny proti neoprávněnému zpřístupnění třetím stranám.**

**Úroveň fyzického a elektronického zabezpečení pro uložení a přenos osobních dat podléhá schválení zaměstnance Ing. Petra Zavadila.**

## Povinnosti zaměstnanců při zpracování osobních údajů

Zaměstnanci organizace mají při zpracování osobních údajů tyto povinnosti:

* povinnost řídit se při zpracování všech osobních údajů, které zpracovávají v rámci výkonu své pracovní náplně v organizaci těmito zásadami ochrany osobních údajů – touto interní směrnicí organizace,
* povinnost zpracovávat **legální a přesné** osobní údaje,
* povinnost zpracovávat osobní údaje pouze **ze zákonných důvodů, za stanoveným účelem** a ve **stanoveném rozsahu** podle rozsahu své pracovní náplně, zaměstnanci jsou povinni zdržet se jakéhokoliv zpracování osobních údajů nad rámec svých pracovních povinností,
* povinnost zpracovávat osobní údaje korektně a transparentně,
* povinnost uchovávat osobní údaje pouze **po dobu nezbytnou** k účelu jejich zpracování, tak jak plyne z příslušného zákona nebo je stanoveno organizací a po uplynutí této doby naložit s nosiči osobních údajů v souladu **se spisovým a skartačním řádem organizace**, uvedené se týká rovněž osobních údajů zpracovávaných v informačních systémech organizace,
* povinnost získání a uchování **výslovného souhlasu** při zpracování zvláštních kategorií údajů a souhlasu při zpracování osobních údajů, které nejsou zpracovány z jiných zákonných důvodů,
* povinnost **informovat a poučit** subjekt údajů o jeho právech a povinnostech ve smyslu čl. 4.5. této směrnice,
* povinnost **dodržovat** přijatá technická a organizační **opatřeník zajištění ochrany** osobních údajů proti jejich zneužití, zejména uchovávat nosiče osobních údajů v uzamykatelných skříních či trezorech, uzamykat místnost při každém odchodu, pravidelně měnit přístupové heslo na svém zařízení a hlásit jakékoliv porušení zabezpečení osobních údajů + pravidlo čistého stolu a obrazovky,
* pro účely transparentního a férového informování všech subjektů údajů o zásadách zpracování osobních údajů v organizaci byl vydán veřejný dokument „**Zásady zpracování osobních údajů**“ který je zveřejněn na viditelném místě web stránek organizace a na který mají všichni zaměstnanci, kteří přichází do styku se subjekty osobních údajů povinnost tyto subjekty odkazovat, a to jak verbálně, tak i písemnou a elektronickou formou, a to zejména v následujících případech:
	+ zasílání e-mailových zpráv – formou upozornění v textaci každého e-mailu,
	+ při předávání jakéhokoli produktu, služby či informace subjektu údajů,
	+ ve všech ostatních případech, kdy není zřejmé, zda byl subjekt údajů o těchto zásadách informován,
* povinnost mlčenlivosti o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i po skončení pracovního poměru v organizaci.

## Práva subjektu údajů

### Právní základ pro zpracování

Správce může zpracovávat osobní údaje pouze zákonným způsobem. Zpracování osobních údajů je dle GDPR zákonné, jestliže:

* je prováděno na základě souhlasu subjektu údajů,
* je nezbytné pro dodržení právní povinnosti správce
* je nezbytné pro splnění smlouvy nebo jednání o smluvních vztazích se subjektem údajů,
* je nezbytné pro účely splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,
* je nezbytné pro účely oprávněných zájmů správce, vyjma případů, kdy mají před těmito zájmy přednost zájmy, práva a svobody subjektu údajů.

### Právo na informace

Základním právem subjektu údajů je právo být informován o totožnosti správce (příp. také o kontaktu na **koordinátora** pro ochranu osobních údajů), dále pak o tom, z jakého důvodu a pro jaké účely budou osobní údaje zpracovány, o rozsahu zpracovaných osobních údajů a o případných příjemcích osobních údajů.

### Právo na přístup

Subjekt údajů má právo na přístup k informacím o zpracování svých osobních údajů. Na základě jeho žádosti je organizace povinna mu tyto informace bez zbytečného odkladu předat, a to ve formě sdělení, které musí obsahovat náležitosti stanovené GDPR. Subjekt údajů má dále právo požadovat po organizaci opravu nepřesných osobních údajů, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů taktéž právo na doplnění svých neúplných osobních údajů.

### Právo na výmaz

Subjekt údajů má za podmínek stanovených v čl. 17, 18 a 21 GDPR právo na výmaz svých osobních údajů, právo na omezení zpracování a právo vznést námitku. Povinností všech zaměstnanců (zejména osob, které přebírají a rozdělují v organizaci doručenou poštu) je v případě obdržení odvolání souhlasu, námitky týkající se zpracování osobních údajů či uplatnění práva subjektu údajů na výmaz či omezení zpracování osobních údajů neprodleně předat tuto informaci **koordinátorovi** pro ochranu osobních údajů.

**Pověřenec/ koordinátor** ve spolupráci se zaměstnanci odpovědnými za zpracování těchto údajů a dalšími pověřenými zaměstnanci organizace provede posouzení oprávněnosti žádosti subjektu údajů a učiní nezbytné kroky dle požadavků GDPR. Firma nemá povinnost jmenovat pověřence pro ochranu osobních údajů.

### Zjištění totožnosti subjektu údajů

**Pověřenec** pro ochranu osobních údajů je při vyřizování jakýchkoli z výše uvedených zákonných nároků subjektu údajů povinnen požadovat po subjektu údajů prokázání totožnosti jedním z následujících způsobů:

* + - * + zasláním písemné žádosti s úředně ověřeným podpisem subjektu údajů,
				+ zasláním elektronické zprávy s platným elektronickým podpisem subjektu údajů,
				+ zasláním zprávy prostřednictvím datové schránky,

a to vždy na zveřejněné kontaktní údaje správce dle platných veřejných zásad.

Firma nemá povinnost jmenovat pověřence. Pokud není jmenován pověřenec, jeho povinnosti je povinna plnit kontaktní osoba. V tomto případě jde o pana Ing. Petra Zavadila.

### Informační povinnost vůči zaměstnancům

Organizace plní vydáním těchto zásad své informační povinnosti správce osobních údajů vůči svým zaměstnancům.

## Zpracování osobních údajů zpracovatelem

V případě, že osobní údaje shromážděné v organizaci jsou zpracovávány jiným subjektem - zpracovatelem, je správce povinen uzavřít s tímto zpracovatelem smlouvu o zpracování osobních údajů, a to v písemné formě. K již existujícím smluvním vztahům správce uzavře smluvní doložku.

Základními náležitostmi smlouvy se zpracovatelem je výslovné uvedení v jakém rozsahu, za jakým účelem a na jakou dobu se smlouva uzavírá, smlouva dále musí obsahovat dostatečné záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů, a to případně i v době po skončení platnosti smlouvy.

Zpracovatel (a jeho pověření zaměstnanci) je zavázán povinností mlčenlivosti ve vztahu ke zpracovaným osobním údajům. Po uplynutí doby (ukončení smlouvy) je zpracovatel povinen provést výmaz všech osobních údajů, které zpracováním získal (vyjma těch osobních údajů, na které se dle příslušných právních předpisů vztahuje povinnost archivace).

Bez předchozího písemného souhlasu organizace zpracovatel rovněž **nesmí** do zpracování zapojit dalšího subjekt provádějící zpracování.

## Postup organizace a zaměstnanců při porušení zabezpečení osobních údajů

Provedením úkonů níže je pověřen Ing. Petr Zavadil.

**Jako koordinátor** je povinna vést dokumentaci všech **událostí** - případů porušení zabezpečení osobních údajů a je povinen ji předložit Úřadu pro ochranu osobních na základě jejich výzvy.

Firma vede evidenci těchto událostí **na icloudu a také na záložním disku.**

### Hlášení událostí s vlivem na ochranu osobních údajů

V případě, že se některý ze zaměstnanců dozví o porušení (popř. hrozbě porušení) zabezpečení osobních údajů v organizaci, je povinen neprodleně tuto událost oznámit **koordinátorce** pro ochranu osobních údajů a poskytnout mu veškeré informace, které se této události týkají.

Evidenci událostí a jejich vyhodnocování zajišťuje Ing. Petr Zavadil.

### Způsob zvládání událostí

**Koordinátor** ve spolupráci se zaměstnanci pověřenými za zpracování osobních údajů, u nichž došlo k porušení zabezpečení těchto údajů, popř. s dalšími zaměstnanci, bez zbytečného odkladu provede šetření s cílem určení míry závažnosti porušení zabezpečení. Zejména prošetří, jakých kategorií osobních údajů se porušení týká, zda a v jakém rozsahu má porušení zabezpečení za následek riziko pro práva a svobody subjektů údajů a zda existuje možnost rychlé nápravy tohoto porušení. Zároveň s příslušnými zaměstnanci přijme nezbytné opatření k nápravě tohoto porušení nebo alespoň ke zmírnění jeho následků.

### Způsob hlášení incidentů

Pokud **koordinátor** po provedeném šetření dospěje k názoru, že porušení zabezpečení osobních údajů má za následek riziko pro práva a svobody subjektů údajů, je povinen tuto skutečnost ohlásit Úřadu pro ochranu osobních údajů, a to ve lhůtě **72 hodin od okamžiku**, kdy se o této skutečnosti některý ze zaměstnanců organizace dozvěděl. Toto ohlášení musí obsahovat alespoň popis povahy daného případu, uvedení kategorií osobních údajů a přibližného množství dotčených subjektů osob a jejich záznamů, jméno a kontakt na pověřence, popis pravděpodobných důsledků a popis provedených opatření k nápravě porušení zabezpečení.

### Oznamování incidentů subjektům údajů

Jestliže porušením zabezpečení osobních údajů může vzniknout vysoké riziko pro práva a svobody fyzických osob (subjektů údajů), je **koordinátor** povinen vhodným způsobem kontaktovat subjekt údajů a oznámit o možném nebezpečí vyplývající z porušení zabezpečení osobních údajů.

# Závěrečná ustanovení

Zaměstnanci organizace odpovídají za dodržování jim stanovených povinností, které se vztahují k ochraně osobních údajů.

Vedení organizace je povinno zajistit prokazatelné seznámení všech svých zaměstnanců organizace s těmito zásadami.