Směrnice
o ochraně osobních údajů

Obsah

Oddíl I. Definice, základní principy, povinnosti a odpovědnosti

1. Úvodní ustanovení

Vedení společnosti TM Stav, spol. s r.o., IČ 48399477, zastoupená jednatelem Martinem Tlaškem (dále jen Společnost), vydává tuto vnitřní normu – Směrnici o ochraně osobních údajů (dále jen směrnice), která stanovuje jednotný soubor pravidel pro zpracování a ochranu osobních údajů v podmínkách Společnosti.

Směrnice vychází ze závazných předpisů a norem, jejichž aktuální seznam je přílohou této směrnice. Primární normou je přitom 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 (dále jen GDPR).

Vzhledem ke komplexnosti problematiky a za účelem usnadnění naplňování požadavků GDPR jsou součástí této směrnice pokyny (návody) pro odpovědné osoby, reagující na typické situace, které mohou v souvislosti se zpracováním a ochranou osobních údajů nastat.

2. Závaznost směrnice

Tato směrnice je závazná pro všechny zaměstnance Společnosti.

Pro subjekty, které realizují zpracování osobních údajů pro Společnost z pozice Zpracovatele, jsou závazná pravidla a principy uvedené ve Smlouvě o zpracování.

3. Definice základních pojmů (dle GDPR)

OSOBNÍ ÚDAJ - veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“). Jedná se například o jméno, identifikační číslo, lokační údaje, síťový identifikátor, biometrické údaje, zdravotní stav atd.

ZPRACOVÁNÍ - jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, které jsou prováděny 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.

OMEZENÍ ZPRACOVÁNÍ - označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu.

PROFILOVÁNÍ - jakákoli 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 pracovního výkonu osoby, její ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.

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.

EVIDENCE - jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.

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.***

ZPRACOVATEL - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který ***zpracovává osobní údaje pro správce***.

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.

TŘETÍ STRANA - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, a který je oprávněn ke zpracování osobních údajů.

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.

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.

BIOMETRICKÝ ÚDAJ - osobní údaj vyplývající z konkrétního technického zpracování a týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, který umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.

ÚDAJ 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.

ZÁSTUPCE - jakákoli fyzická nebo právnická osoba usazená v EU, 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.

PODNIK - jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost.

SKUPINA PODNIKŮ - skupina zahrnující řídící podnik a jím řízené podniky.
Závazná podniková pravidla - koncepce ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel usazený na území členského státu EU 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.

DOZOROVÝ ÚŘAD - nezávislý orgán veřejné moci zřízený členským státem podle článku 51 GDPR, v případě ČR jde o Úřad na ochranu osobních údajů.

PŘESHRANIČNÍ ZPRACOVÁNÍ - a) zpracování osobních údajů, které probíhá v souvislosti s činnostmi provozoven ve více než jednom členském státě správce či zpracovatele v EU, 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 EU, ale kterým jsou nebo pravděpodobně budou podstatně dotčeny subjekty údajů ve více než jednom členském státě EU.

RELEVANTNÍ A ODŮVODNĚNÁ NÁMITKA - 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. Relevantní a odůvodněná námitka jasně dokazuje významnost rizik vyplývajících z návrhu rozhodnutí, pokud jde o základní práva a svobody subjektů údajů, případně o volný pohyb osobních údajů v rámci EU.

V případě nejasnosti či nezbytnosti vymezení dalších pojmů lze využít plné znění GDPR.

4. Základní zásady zpracování osobních údajů

Osobní údaje musí být:

- zpracovávány korektně a zákonným a transparentním způsobem (***zásady zákonnosti, korektnosti a transparentnosti***),
- shromažďovány pro určité, výslovně vyjádřené a legitimní účely; současně nesmějí být zpracovávány způsobem, který je s těmito účely neslučitelný (***zásada omezení účelem***),

- přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány (***zásada minimalizace údajů***),
- přesné a v případě potřeby aktualizované (***zásada přesnosti***),
- 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, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných GDPR s cílem zaručit práva a svobody subjektu údajů (***princip omezení uložení***),
- 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 (***zásada zajištění integrity a důvěrnosti***).

Správce odpovídá za dodržení svých povinností a musí být schopen toto dodržení souladu doložit (***zásada odpovědnosti***).

5. Zákonnost zpracování

Zpracování osobních údajů je možné výhradně na základě následujících právních titulů (za dodržení základních principů a zásad):

- subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů,
- 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,
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,
- 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.

6. Souhlas se zpracováním osobních údajů

Jestliže je právním titulem zpracování souhlas subjektu údajů, musí být ***správce schopen doložit***, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů.

Pokud je souhlas 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.

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.

Pokud se použije výše uvedených ustanovení 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.

Zvláštní kategorie osobních údajů

Osobními údaji náležejícími do Zvláštní kategorie osobních údajů jsou osobní údaje, které vypovídají o:

- rasovém či etnickém původu,
- politických názorech,
- náboženském vyznání či filozofickém přesvědčení,
- členství v odborech,
- zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby,
- zdravotním stavu,
- sexuálním životě nebo sexuální orientaci fyzické osoby.

Obecně je dle GDPR zpracování výše uvedených údajů zakázáno, pakliže není splněna některá z následujících výjimek:

- subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů,
- zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem EU nebo jejího členského státu nebo kolektivní dohodou podle práva členského státu,
- zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas,
- zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy

tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt,

- zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů,
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí,
- zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva EU nebo jejího členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů,
- zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva EU nebo jejího členského státu nebo podle smlouvy se zdravotnickým pracovníkem,
- zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva EU nebo jejího členského státu,
- zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.

Zvláštní ustanovení o osobních údajích v trestních věcech

Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření se může provádět pouze pod dozorem orgánu veřejné moci nebo pokud je oprávněné podle práva EU nebo jejího členského státu poskytujícího vhodné záruky, pokud jde o práva a svobody subjektů údajů.

7. Práva subjektu údajů

Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem, za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v příslušných ustanoveních GDPR.

Informace poskytne písemně nebo jinými prostředky, případně v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.

Správce neodmítne vyhovět žádosti subjektu údajů za účelem výkonu jeho práv dle příslušných ustanovení GDPR, ledaže doloží, že nemůže zjistit totožnost subjektu údajů.

Správce poskytne subjektu údajů na žádost podle článků 15 až 22 GDPR informace o přijatých opatřeních, a to bez zbytečného odkladu a v ***každém případě do jednoho měsíce od obdržení žádosti***. Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další dva měsíce. Správce informuje subjekt údajů o jakémkoliv takovém prodloužení do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad.

Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, je-li to možné, pokud subjekt údajů nepožádá o jiný způsob.

Pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti subjekt údajů o důvodech nepřijetí opatření a o možnosti podat stížnost u dozorového úřadu a žádat o soudní ochranu.

Informace podle článků 13 a 14 GDPR a veškerá sdělení a veškeré úkony podle článků 15 až 22 a 34 GDPR **se poskytují a činí bezplatně**.

Jsou-li žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může správce buď: a) uložit přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo sdělení nebo s učiněním požadovaných úkonů; nebo b) odmítnout žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost žádosti dokládá správce.

Právo na poskytnutí informací

V případě, že správce získává osobní údaje přímo od subjektu údajů, je povinen v okamžiku získání osobních údajů subjektu údajů poskytnout tyto informace:

- totožnost a kontaktní údaje správce a jeho případného zástupce,
- kontaktní údaje pověřence pro ochranu osobních údajů (pokud je jmenován),
- účely zpracování, pro které jsou osobní údaje určeny a právní základ pro zpracování,
- oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno právním titulu oprávněného zájmu,
- případné příjemce nebo kategorie příjemců osobních údajů,
- případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci.

Pokud je to nezbytné pro zajištění spravedlivého a transparentního zpracování, poskytne správce dále ještě tyto informace:

- doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby,

- existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů,
- pokud je zpracování založeno na souhlasu nebo výslovném souhlasu existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním,
- existence práva podat stížnost u dozorového úřadu,
- skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů,
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.

Pokud správce hodlá osobní údaje **dále zpracovávat pro jiný účel**, než je účel, pro který byly shromážděny, poskytne subjektu údajů **ještě před uvedeným dalším zpracováním** informace o tomto jiném účelu a příslušné další informace – viz výše.
Informace poskytované subjektu údajů v případě, že nebyly získány přímo od subjektu údajů upravuje Článek 14 GDPR.

Právo na přístup k osobním údajům

Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou správcem zpracovávány.

V případě, že osobní údaje správcem zpracovávány jsou, má subjekt údajů právo na následující informace:

- účely zpracování,
- kategorie dotčených osobních údajů,
- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
- plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby,
- existence práva požadovat od správce opravu nebo výmaz osobních údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování,
- právo podat stížnost u dozorového úřadu,
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.

Pokud se osobní údaje předávají do třetí země nebo mezinárodní organizaci, má subjekt údajů právo být informován o vhodných zárukách.

Správce je povinen poskytnout na základě žádosti kopii zpracovávaných osobních údajů, a to v listinné nebo elektronické podobě, dle charakteru žádosti (u elektronické podoby ve standardním čitelném formátu).

Právem získat kopii nesmějí být nepříznivě dotčena práva a svobody jiných osob.

Právo na opravu

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají.

Právo na výmaz

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování,
- subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
- osobní údaje byly zpracovány protiprávně,
- osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu EU nebo jejího členského státu, které se na správce vztahuje,
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1 GDPR.

Jestliže správce osobní údaje zveřejnil, a je povinen je z výše uvedených důvodů vymazat, přijme **s ohledem na dostupnou technologii a náklady na provedení** přiměřené kroky, včetně technických opatření, aby informoval správce, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.

Konkrétní důvody pro vyloučení práva na výmaz je zpracování nezbytné pro:

- výkon práva na svobodu projevu a informace,
- splnění právní povinnosti, jež vyžaduje zpracování podle práva EU nebo jejího členského státu splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci,
- z důvodů veřejného zájmu v oblasti veřejného zdraví,
- účely archivace ve veřejném zájmu,
- účely vědeckého či historického výzkumu či pro statistické účely,

- pokud je pravděpodobné, že by právo na výmaz znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování,
- určení, výkon nebo obhajobu právních nároků.

Právo na omezení zpracování

Subjekt údajů má právo na to, aby správce omezil zpracování, pokud:

- subjekt údajů popírá přesnost osobních údajů,
- zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití,
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků,
- subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

Pokud bylo zpracování omezeno, mohou být tyto osobní údaje - s výjimkou jejich uložení - zpracovány pouze se souhlasem subjektu údajů nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu EU nebo některého jejího členského státu.

Právo na přenositelnost údajů (portabilitu)

Subjekt údajů má právo získat osobní údaje (jež poskytl správci) ve strukturovaném, běžně používaném a strojově čitelném formátu, a tyto údaje předat jinému správci.

Právo na přenositelnost je možno uplatnit pokud:

- je zpracování založeno na souhlasu,
- je zpracování založeno na smlouvě,
- zpracování se provádí automatizovaně.

Právem nesmí být nepříznivě dotčena práva a svobody jiných osob.

Právo vznést námitku

Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů na základě těchto právních titulů:

- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,

- zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany.

Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů.

Pokud se osobní údaje zpracovávají pro účely **přímého marketingu**, má subjekt údajů právo vznést kdykoli námitku proti zpracování osobních údajů, které se ho týkají, pro tento marketing, což zahrnuje i profilování, pokud se týká tohoto přímého marketingu. Pokud subjekt údajů vznese námitku proti zpracování pro účely přímého marketingu, nebudou již jeho osobní údaje pro tyto účely zpracovávány.

Právo nebýt předmětem automatizovaného rozhodování

Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.

Konkrétní podmínky a výjimky stanovuje Článek 22 GDPR.

8. Odpovědnosti a povinnosti

Odpovědnost a povinnosti správce

Správce s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob **zavede vhodná technická a organizační opatření**, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s GDPR. Tato opatření musí být podle potřeby **revidována a aktualizována.**

Správce zavede vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti **(zásada minimalizace zpracovávaných údajů)**.

Společní správci mezi sebou transparentním ujednáním vymezí své podíly na odpovědnosti za plnění povinností dle GDPR.

Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá. Záznamy obsahují tyto informace:

- jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů,

- účely zpracování,
- popis kategorií subjektů údajů a kategorií osobních údajů,
- kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích,
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace,
- je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů,
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.

Správce, zpracovatel nebo případný zástupce správce nebo zpracovatele poskytne záznamy na požádání dozorového úřadu.

Odpovědnost a povinnosti zpracovatele

Pokud má být zpracování provedeno pro správce, využije správce pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky GDPR a aby byla zajištěna ochrana práv subjektu údajů.

Zpracovatel nesmí do zpracování zapojit žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce.

Zpracování zpracovatelem se **řídí smlouvou nebo jiným právním aktem** podle práva EU nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce.

Konkrétní podrobnosti stanovuje Článek 28 GDPR.

Každý zpracovatel a jeho případný zástupce vede záznamy o všech kategoriích činností zpracování prováděných pro správce, jež obsahují:

- jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná (včetně zástupců a pověřenců),
- kategorie zpracování prováděného pro každého ze správců,
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace,
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.

9. Bezpečnost zpracování

S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku.

Možnými (nikoliv povinnými) způsoby zajištění jsou mj.:

- pseudonymizace a šifrování osobních údajů,
- schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,
- schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů,
- proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

10. Hlášení bezpečnostních incidentů

Bezpečnostním incidentem se rozumí případ porušení zabezpečení osobních údajů. Lze jej definovat jako jakékoli porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených anebo jinak zpracovávaných osobních údajů.

Porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno **do 72 hodin** od okamžiku, kdy se o něm dozvěděl**, ohlásí příslušnému dozorovému úřadu.** Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

Správce není povinen učinit ohlášení, pokud je nepravděpodobné, že by zjištěné porušení mělo za následek riziko pro práva a svobody fyzických osob.

Pokud zjistí porušení zabezpečení osobních údajů **zpracovatel, ohlásí** je bez zbytečného odkladu **správci**.

Ohlášení musí přinejmenším obsahovat:

- popis povahy daného případu porušení zabezpečení osobních údajů, včetně - pokud je to možné - kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů,
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace,
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů,

- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Správce **dokumentuje veškeré případy porušení zabezpečení osobních údajů**, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem.

Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu také subjektu údajů.

Případné podrobnosti stanovuje GDPR.

Posouzení vlivu na ochranu osobních údajů

Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude mít - s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování - za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.

Při provádění posouzení vlivu na ochranu osobních údajů si správce vyžádá posudek pověřence pro ochranu osobních údajů, byl-li jmenován.

Povinnost provést posouzení vlivu na soukromí stanovuje GDPR zejména v těchto případech:

- systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,
- rozsáhlé zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených,
- rozsáhlé systematické monitorování veřejně přístupných prostorů.

Obsah posouzení stanovuje GDPR, přičemž správce jej provádí na základě interní metodiky.

Správce konzultuje před zpracováním s dozorovým úřadem, pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že by dané zpracování mělo za následek **vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika.**

Další podrobnosti stanovuje GDPR.

Pověřenec pro ochranu osobních údajů

Konkrétní podmínky a důvody pro jmenovaní pověřence pro ochranu osobních údajů stanovuje GDPR.

Pověřenec pro ochranu osobních údajů musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit stanovené úkoly. Pověřenec pro ochranu osobních údajů může být pracovníkem správce či zpracovatele, nebo může úkoly plnit na základě smlouvy o poskytování služeb.

Správce nebo zpracovatel zveřejní kontaktní údaje pověřence pro ochranu osobních údajů a sdělí je dozorovému úřadu.

11.Ostatní ustanovení

Školení a vzdělávání

Školení a vzdělávání uživatelů v oblasti týkající se ochrany osobních údajů zajišťuje a garantuje správce, a to vlastními silami nebo pomocí externích subjektů. Spolupráce s externími subjekty vyžaduje schválení vedením Společnosti.

Kontrola a opatření k nápravě

Pro vyhodnocení skutečného stavu plnění ustanovení této směrnice, jakož i konkrétních požadavků GDPR, správce ve spolupráci s určenou osobou provádí periodickou kontrolu dodržování příslušných ustanovení, a to v rozsahu nejméně 2 x ročně. Kontrolní činnost může být doplněna nezávislým auditem či posouzením.

O kontrolách a jejich výsledcích jsou vedeny záznamy, uchovávané vedením Společností.

Kontrolní činností není dotčena periodicita jednotlivých opatření a úkolů, které vychází z povinností dle GDPR.

Opatření k nápravě

Správce na základě zjištěných nedostatků přijímá neprodleně příslušná technická nebo organizační opatření, ev. jiná opatření k nápravě.

12.Odpovědnost zaměstnanců

Opatření vyplývající z porušení této směrnice uživatelem je opatřením z důvodu porušení povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci (Zákoník práce) a přijímá ho osoba s personální pravomocí.

Odpovědnost zaměstnance za škodu vzniklou v souvislosti s porušením bezpečnosti osobních údajů, jakož i odpovědnost za porušení GDPR, se řídí obecně platnými právními předpisy.

Oddíl II. Postupy

1. Postup pro hlášení případů porušení zabezpečení osobních údajů dle GDPR (bezpečnostních incidentů).

Bezpečnostním incidentem se rozumí jakékoli porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

Příklady

Příkladem ztráty osobních údajů může být ztráta flash disku obsahující kopii správcovy databáze zákazníků nebo zaměstnanců, kterou někdo ztratil nebo ukradl. Dalším příkladem je zašifrování osobních údajů vyděračským softwarem (ramsomware), bez možnosti k těmto údajům získat jiný přístup. Obdobně lze nahlížet na incident, kdy dojde k odeslání nezajištěných výplatních pásek na několik e-mailů, které nepatří danému zaměstnanci. Ztráta dostupnosti může nastat v případě vážného narušení normálních chodu společnosti, například při výpadku elektřiny, či útoku z kybernetické sítě (např. DDoS). Častým incidentem může být odcizení nebo ztráta notebooku, který obsahuje osobní údaje zaměstnanců, zákazníků apod. Nejinak je tomu u „chytrých“ mobilních telefonů, které obsahují telefonní seznamy, e-maily atd.

Každý zaměstnanec, který zjistí porušení zabezpečení osobních údajů (i pokud si není jistý, že se jedná o porušení), **bez jakéhokoliv prodlení vyrozumí o této skutečnosti osobu odpovědnou za ochranu osobních údajů a vedení Společnosti.**

Osoba odpovědná za ochranu osobních údajů ve spolupráci s vedením Společnosti postupuje dle následujícího schématu:

Schéma postupu oznámení

(v případě nejistoty v postupu kontaktuje osoba odpovědná za ochranu osobních údajů právní kancelář nebo bezpečnostního konzultanta)

Příklady porušení zabezpečení a komu oznamovat (dle vodítka WP29)

Příklad	Ohlásit dozorovému úřadu?	Oznámit subjektu údajů?	Poznámky/doporučení
I. Správce uložil záložní kopii archivu osobních údajů v zašifrované podobě na CD. Toto CD bylo odcizeno vloupáním.	Ne.	Ne.	Pokud jsou data zašifrovaná pomocí algoritmu na úrovni doby, data jsou zálohovaná a jedinečný klíč nebyl prozrazen, pak nemusí jít o hlásitelný případ. Jsou-li však později klíč a šifrování prolomeny, ohlášení je nutné.
II. Osobní údaje jednotlivců jsou vyfiltrovány z bezpečné webové stránky provozované správcem během kybernetického útoku. Správce má zákazníky jen v jednom členském státě.	Ano, ohlásit případ příslušnému dozorovému úřadu je třeba, pokud hrozí možné důsledky pro jednotlivce.	Ano, oznámení jednotlivcům je nutné v závislosti na povaze dotčených osobních údajů a v případě vysoké závažnosti případných dopadů na jednotlivce.	Není-li riziko vysoké, doporučujeme, aby správce informoval subjekt údajů podle okolností případu. Oznámení například nemusí být vyžadováno, pokud jde o porušení důvěrnosti při zasílání novinek týkajících se televizní estrády, avšak může být nutné, pokud newsletter (zpravodaj) může vést k rozpoznání politických názorů subjektu údajů.
III. Krátký, jen několikaminutový výpadek proudu ve správcově call centru způsobí, že se s ním zákazníci nemohou spojit a získat přístup ke svým záznamům.	Ne.	Ne.	Nejedná se o porušení zabezpečení osobních údajů, které by bylo nutno ohlašovat, ale pořád je to incident, který je potřeba dokumentovat podle článku 33, odst. 5. Správce by měl vést náležité záznamy.
IV. Správce utrpí útok ransomwarem (vyděračským softwarem), čímž dojde k zašifrování všech jeho dat. K dispozici nejsou žádné zálohy a data nelze obnovit. Během šetření se přijde na to, že jedinou schopností ramsomwaru bylo zašifrování údajů, a že systém neobsahoval žádný jiný škodlivý software (malware).	Ano, ohlásit případ příslušnému dozorovému úřadu je nutné, pokud hrozí možné důsledky pro jednotlivce, neboť se jedná o ztrátu dostupnosti.	Ano, nutnost oznámit případ jednotlivcům bude záviset na povaze dotčených osobních údaj a na možných dopadech ztráty dostupnosti, jakož i na dalších pravděpodobných důsledcích.	Pokud by existovala záložní kopie a data by bylo možno v přijatelném čase obnovit, pak nebude třeba ohlašovat dozorovému úřadu ani oznamovat jednotlivci, protože by se nejednalo o trvalou ztrátu dostupnosti nebo důvěrnosti. Dozorový úřad však může zvážit provedení šetření k posouzení souladu s obecnějšími požadavky stanovenými v článku 32.

Příklad	Ohlásit dozorovému úřadu?	Oznámit subjektu údajů?	Poznámky/doporučení

V. Jednotlivec zavolá call centrum banky, aby ohlásil případ porušení zabezpečení. Volající totiž obdržel měsíční výpis z účtu někoho jiného. Správce zahájí krátké šetření (tj. ukončené např. během 24 hodin) a s dostatečnou jistotou zjistí, že došlo k porušení zabezpečení osobních údajů a že se jedná o systémovou chybu, takže i další jednotlivci byli nebo by mohli být postiženi.	Ano.	Potřeba je oznámit to pouze dotčeným jednotlivcům za předpokladu, že existuje vysoké riziko a je jasné, že nikdo další nebyl zasažen.	Pokud bude dalším šetřením zjištěno, že bylo postiženo více osob, ohlášení dozorovému úřadu musí být učiněno a správce také musí záležitost dodatečně oznámit příslušným dalším jednotlivcům, existuje-li vysoké riziko.
Příklad	**Ohlásit dozorovému úřadu?**	**Oznámit subjektu údajů?**	**Poznámky/doporučení**
VI. Nadnárodní online tržiště se stane obětí kybernetického útoku, přičemž útočník na internetu zveřejní uživatelská jména, hesla a nákupní historii.	Ano, ohlášení dozorovému úřadu je nutné, týká-li se případů přeshraničního zpracování.	Ano, protože uvedený incident by mohl mít za následek vysoké riziko.	Správce by měl podniknout okamžité kroky, např. vynutit resetování hesel u dotčených účtů, a učinit i další opatření ke snížení rizika.
VII. Webhostingová firma (zpracovatel) zjistí chybu v kódu, který sleduje uživatelská oprávnění. Následkem této chyby může jakýkoliv uživatel vstoupit do účtu kteréhokoliv jiného uživatele.	Webhostingová firma, jsouce v postavení zpracovatele, musí věc bezodkladně ohlásit dotčeným klientům (správcům). Za předpokladu, že webhostingová firma provedla vlastní šetření, měli by mít dotčení správci důvodnou jistotu, zda každý z nich byl zasažen porušením, a tedy se o případu „dozvěděl“ ve chvíli, kdy byl informován webhostingovou firmou (zpracovatelem). Správce pak musí případ ohlásit dozorovému úřadu.	Pokud není pravděpodobné, že by se mohlo objevit vysoké riziko pro jednotlivce, není potřeba subjektům údajů případ oznámit.	Webhostingová firma (zpracovatel) musí vzít v úvahu veškeré další oznamovací povinnosti (např. podle Směrnice NIS). Neexistuje-li důkaz, že u konkrétního správce nebylo daného zranitelného místa zneužito, pak nemuselo dojít k porušení, které by bylo třeba ohlásit. Přesto by incident měl být dokumentován a považován za záležitost, která je v nesouladu s článkem 32.
VIII. Zdravotní záznamy v nemocnici nejsou dostupné po dobu 30 hodin v důsledku kybernetického útoku.	Ano, nemocnice je povinna tento incident ohlásit, vzhledem k vysokému riziku pro pacientovo zdraví a soukromí.	Ano, je třeba provést oznámení dotčeným jednotlivcům.	
Příklad	**Ohlásit dozorovému úřadu?**	**Oznámit subjektu údajů?**	**Poznámky/doporučení**

IX. Osobní údaje 5000 studentů byly omylem zaslány na nesprávný adresář čítající 1000 a více příjemců.	Ano, ohlásit případ dozorovému úřadu je nutné.	Ano, nutnost oznámení jednotlivcům bude záviset na rozsahu a druhu dotčených osobních údajů a na závažnosti možných důsledků.	
X. E-mail v rámci přímého marketingu byl odeslán příjemcem v kolonce „komu“ nebo „kopie“, čímž každý z příjemců mohl zjistit elektronickou adresu ostatních příjemců.	Ano, ohlášení dozorovému úřadu může být povinné, jestliže byl postižen velký počet jednotlivců, došlo k odhalení citlivých údajů (např. adresář psychoterapeuta) nebo pokud existují jiné faktory představující vysoké riziko (např. zpráva obsahuje iniciační hesla).	Ano, nutnost oznámení jednotlivcům bude záviset na rozsahu a druhu dotčených osobních údajů a na závažnosti možných důsledků.	Ohlášení nemusí být nutné, pokud nedošlo k odhalení „citlivých údajů“ a pokud došlo k odkrytí jen menšího počtu e-mailových adres.

2. Postupy pro plnění práv subjektů

Správce osobních údajů je povinen informovat subjekty údajů (nositele osobních údajů) o jejich právech a zároveň plně umožnit plnění těchto práv.

Správce poskytuje rovněž kontaktní údaje, pomocí nichž lze s požadavkem na plnění práva správce kontaktovat.

V souladu s principy a povinnostmi dle GDPR správce zajistí odpověď na požadavek subjektu údajů bez zbytečného odkladu, a to **nejpozději do jednoho měsíce od obdržení žádosti**. Ve výjimečných případech může být tato lhůta prodloužena (viz GDPR).

Konkrétní práva subjektů jsou definována v Oddíle I. této směrnice.

Společný postup pro splnění požadavků v souvislosti s plněním práv subjektů:

Přijetí žádosti

Správce přijímá žádosti způsobem, který deklaruje v politice zpracování osobních údajů, zpravidla tedy osobně, poštovními službami vč. datové schránky, e-mailem, telefonicky, případně jinak uzpůsobeným kanálem pro přijímání žádostí tohoto charakteru.

Každý zaměstnanec, který přijme žádost, ji bezodkladně předá osobě odpovědné za ochranu osobních údajů, případně vedení Společnosti.

Vyhodnocení žádosti

Osoba odpovědná za ochranu osobních údajů vždy nejprve ověří totožnost žadatele. Bez ověření totožnosti nelze na požadavek reagovat.

Ověření totožnosti představuje u osobního požadavku předložení dokladu totožnosti k nahlédnutí, u datové schránky je totožnost odesilatele verifikována samotnou službou, u ostatních požadavků je nezbytné vyzvat žadatele k tomu, aby svou totožnost v rámci požadavku prokázal (zaslal žádost cestou datové schránky, dostavil se osobně, zaslal žádost s ověřeným podpisem apod.).

Po ověření totožnosti osoba odpovědná za ochranu osobních údajů posoudí obsah žádosti, přičemž se při tomto posouzení zabývá stránkou obsahovou, nikoliv názvem žádosti. Po vyhodnocení druhu žádosti přistoupí k plnění požadavku, a to za spolupráce příslušných zaměstnanců či vedení Společnosti.

Plnění požadavku

Osoba odpovědná za ochranu osobních údajů koordinuje činnosti nezbytné pro splnění požadavků (s ohledem na konkrétní povinnost). Například v případě uplatnění práva na přístup ověří, zda jsou osobní údaje žadatele zpracovávány (personalistka, správce informačního systému, marketing atd.) a požádá dotyčné osoby o sdělení rozsahu zpracování a dalších parametrů – viz Oddíl I. směrnice.

I při uplatnění jiných práv spolupracuje vždy osoba odpovědná za ochranu osobních údajů s ostatními odpovědnými zaměstnanci (IT správce, personalistka, management atd.).

Plnění v případě nejistoty

Pokud si osoba odpovědná za ochranu osobních údajů není jistá obsahem žádosti či jejím plněním, bez zbytečného odkladu si vyžádá stanovisko právní kanceláře nebo stanovisko bezpečnostního konzultanta.

Splnění požadavku

Po zajištění veškerých potřebných podkladů osoba odpovědná za ochranu osobních údajů vypracuje písemnou odpověď, případně zajistí předávané materiály (například při uplatnění práva na přenositelnost zajistí nosič s osobními údaji v požadovaném formátu apod.).
Následně zajistí předání odpovědi či materiálů, a to takovým způsobem, aby nemohlo dojít k ohrožení samotných osobních údajů či předávaných informací. V praxi to znamená předání pomocí zajištěného komunikačního kanálu, tedy doporučenou poštou, datovou schránkou, osobně oproti podpisu, v šifrované podobě mailem apod.

Kopii odpovědi, včetně potvrzení o doručení, odeslání či předání, založí do příslušné dokumentace (např. šanon plnění práv subjektů).

Rovněž poznačí či zvýrazní přesné datum plnění práva.

Příklady:

Příklad	**Popis řešení**
Bývalý zaměstnanec se dostaví osobně do Společnosti s tím, že chce uplatnit právo na výmaz (být zapomenut).	Osoba odpovědná za ochranu osobních údajů ověří totožnost žadatele, zaeviduje žádost. Ve spolupráci s odpovědnými osobami zajistí, pro jaké účely, v jakém rozsahu, z jakých právních důvodů atd. jsou osobní údaje bývalého zaměstnance zpracovávány. Pokud je možno uplatnit právo pro některá konkrétní zpracování např. fotografie na firemním facebooku, zajistí technické provedení výmazu. U údajů, které jsou zpracovávány na základě řádných právních titulů a účelů (např. právní povinnost uchovávat pro účely FÚ, soc. pojištění atd.) pouze informuje, po jakou dobu ještě bude probíhat zpracování. Následně vypracuje odpověď žadateli, ve které informuje, které osobní údaje byly vymazány a které budou nadále zpracovávány, s odůvodněním, proč tomu tak je, jaký je účel, právní titul, rozsah a po jakou dobu bude zpracování nadále realizováno.
Zákazník se osobně dostaví do Společnosti a žádá využití práva na přenositelnost (portabilitu), přičemž si chce přenést údaje o nákupech z e-shopu k jinému poskytovateli.	Osoba odpovědná za ochranu osobních údajů ověří totožnost žadatele, zaeviduje žádost. U správce E-shopu ověří, že požadované informace jsou u daného zákazníka k dispozici. Poté ve spolupráci se správcem IT zajistí přenesení údajů ve strojově čitelném formátu (např. CSV, XLSX) na médium, které umožňuje přenesení (CD, flash disk, paměťová karta apod.). Vypracuje odpověď a zajistí předání požadovaných údajů zákazníkovi (oproti podpisu). Kopii zprávy s podpisem zákazníka o převzetí založí do příslušné administrativní pomůcky.
Kdokoliv zašle e-mailem žádost o přístup ke svým osobním údajům.	Osoba odpovědná za ochranu osobních údajů vyzve žadatele, aby hodnověrným způsobem ověřil svou totožnost, například zasláním e-mailu s certifikovaným podpisem, cestou datové schránky, zastavil se osobně (ev. jinak hodnověrným způsobem). Zákazník zašle e-mail s elektronickým podpisem. Osoba odpovědná za ochranu osobních údajů ověří u odpovědných osob dle záznamu o zpracování, zda jsou k žadateli zpracovávány osobní údaje, v jakém rozsahu, za jakým účelem, na základě právního titulu atd. Následně vypracuje odpověď a zašle ji e-mailem s elektronickým podpisem zpět žadateli. Kopii s informací o doručení nebo převzetí založí do příslušné administrativní pomůcky.

3. Postupy pro zajištění bezpečnosti osobních údajů

S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel **vhodná technická a organizační opatření**, aby zajistili úroveň zabezpečení odpovídající danému riziku.

Ke splnění povinností dle GDPR určuje Správce zejména tato pravidla:

- správce vydává a vymáhá závazná pravidla pro oblast informační bezpečnosti, zejména pak stanovuje politiku bezpečnosti pro informační a komunikační technologie,
- veškeré listinné písemnosti obsahující osobní údaje musí být v nepřítomnosti pověřených osob zabezpečeny v uzamykatelných skříních či uzamykatelných prostorách (např. samostatná kancelář), ev. na jiných zabezpečených místech tak, aby byla zajištěna jejich náležitá ochrana. Není přitom rozhodující, zda se jedná o originální písemnosti či zhotovené kopie,
- veškeré osobní údaje v elektronické podobě (v rámci IS i jako nestrukturovaná data na jednotlivých zařízeních) musí být vhodným způsobem zabezpečeny, a to zejména s ohledem na řízení přístupu (kdo konkrétně může přistupovat – vlastní účet, heslo, role, oprávnění), zajištění fyzického přístupu k zařízení a dalších opatření, která jsou definována politikou informační bezpečnosti.

Odpovědnost za dodržování nastavených pravidel, postupů a norem nese každý zaměstnanec, který zpracovává osobní údaje v jakékoliv podobě. Technická opatření bezpečnosti zajišťuje IT správce nebo jiná vedením pověřená osoba.

Závěrečná ustanovení

Tato norma podléhá pravidelné revizi, nejméně pak jednou ročně.

Směrnice nabývá účinnosti dnem 25. 5. 2018.

Za společnost

.....

Příloha č. 1 – Přehled důležitých právních norem

Nařízení Evropského parlamentu a Rady (EU):

Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR)

Zákony:

Z. č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

Z. č. 89/2012 Sb., občanský zákoník

Z. č. 40/2009 Sb., trestní zákoník

Interní normy:

Bezpečnostní politika společnosti

Směrnice pro užívání IKT

Role a odpovědnosti

Role	Odpovědnosti:
Osoba odpovědná za problematiku ochrany osobních údajů	Pravidelná revize normy, návrhy na její doplnění. Kontrola dodržování formálních a administrativních kroků. Kontrola existence záznamů dle této normy. Vyhodnocení, šetření, řešení, ohlašování bezpečnostních incidentů. Reakce a koordinace na požadavky související s uplatněním práv subjektů. Průběžné informování vedení Společnosti. Konzultace s odbornou autoritou. Spolupráce s dozorovým úřadem (UOOU).
Ředitelé, vedoucí pracovníci	Nastavení, dodržování a dohled nad plněním povinností dle této směrnice a GDPR. Kontrolní činnost – plnění uložených úkolů, obecných povinností (v rámci vlastní sekce). Organizace vzdělávání v oblasti ochrany osobních údajů.
Právní oddělení (Bezpečnostní partner nebo Advokátní kancelář)	Přehled o aktuální legislativních změnách. Poskytnutí právní pomoci, právní garance atd. Poskytnutí součinnosti při řešení bezpečnostních incidentů.
Všichni zaměstnanci	Zpracování osobních údajů v souladu se směrnicí. Dohled nad osobními údaji tak, aby bylo minimalizováno riziko ztráty, prozrazení, změny, poškození a zneužití. Hlášení bezpečnostních incidentů nadřízených a určeným osobám.
Personální oddělení	Přijímání personálních opatření ve vztahu k porušení uložených povinností zaměstnanců ev. ve spolupráci s právní kanceláří. Koordinace činností při ukončení pracovního poměru. Plnění pokynů osoby odpovědné za ochranu osobních údajů (pokyny, požadavky, úkoly atd.).
Všichni	Dodržování všech stanovených zásad, povinností a odpovědností.