	Označení dokumentu: **SM - 46**	Verze č.: 1	Platí od: 1.5.2018
MONTPROJEKT	Název dokumentu: **Směrnice o ochraně osobních údajů**		

Obsah

	Funkce	Jméno	Datum	Podpis
Zpracoval	Ekonom	Šárka Dvořáková	01.05.2018	
Schválil	Ředitel	Jaromír Kopic	01.05.2018	

Přezkoumal	TOQUM s.r.o.	Pavel Rychlík	01.05.2018	

1 Obecně

1.1 Účel

Účelem této směrnice je vytvořit rámec standardů a postupů týkajících se ochrany osobních údajů fyzických osob v rámci společnosti.

1.2 Rozsah působnosti

Tato směrnice je platná pro všechny zaměstnance společnosti.

1.3 Kompetence a odpovědnost

Základní odpovědnost za provádění činností dle této směrnice má ředitel společnosti.

1.4 Definice pojmů

Jednotlivé pojmy jsou definovány v bodu 2.1. – osobní údaj, zvláštní kategorie osobních údajů, subjekt údajů, zpracování osobních údajů, správce, zpracovatel, žadatel, příjemce, třetí osoba, oprávněná osoba, princip „Need to know“, automatizované zpracování osobních údajů, pseudonymizace, nosič informací, informace, dokument, zveřejněný osobních údaj, evidence/katalog, zvláštní právní předpis.

1.5 Seznam zkratek

Úřad – úřad pro ochranu osobních údajů

Zákon – Legislativa ČR

Nařízení – Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES

ŘS – ředitel společnosti

2 Obecné zásady ochrany osobních údajů

2.1 Vysvětlení jednotlivých pojmů

Osobní údaj

Veškeré informace o identifikovaném nebo identifikovatelném subjektu údajů; identifikovatelným subjektem údajů 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. Jedná se o příkladný výčet.

Zvláštní kategorie osobních údajů

Zvláštní kategorie osobních údajů jsou osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické údaje nebo biometrické údaje jedinečně identifikující subjekt

údajů a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci subjektu údajů, dále také jako „**zvláštní osobní údaje**“.

Subjekt údajů
Fyzická osoba, k níž se osobní údaje vztahují a která je na základě těchto údajů identifikovatelná, může se jednat o zaměstnance, klienta/uživatele, návštěvníka objektu atd.

Zpracování osobních údajů

Jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, které je prováděno 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, likvidace nebo zničení.

Správce

Každý subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Zpracováním osobních údajů může Organizace jako Správce zmocnit nebo pověřit Zpracovatele, pokud zvláštní zákon nestanoví jinak.

Zpracovatel
Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro Správce.

Žadatel

Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který Organizaci doručí žádost týkající se osobních údajů subjektů údajů.

Příjemce
Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterému jsou osobní údaje ze strany Organizace poskytnuty, ať už se jedná o třetí osobu, či nikoli. Orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu se zvláštními právními předpisy, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany osobních údajů pro dané účely zpracování.

Třetí osoba
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.

Oprávněná osoba
Fyzická nebo právnická osoba, která je oprávněna seznámit se s osobním údajem.

Princip „Need to know“
Objektivní a důvodná potřeba na straně oprávněné osoby seznámit se s osobním údajem za účelem plnění pracovních povinností či jiných povinností nebo oprávněných zájmů.

Automatizované zpracování osobních údajů
Operace uskutečňované zcela nebo zčásti pomocí automatizovaných postupů, zahrnuje operace typu: ukládání osobních údajů na nosiče informací, provádění logických a/nebo aritmetických operací s těmito osobními údaji, jejich změna, likvidace, vyhledávání nebo rozšiřování. Na základě této definice pak lze dospět k závěru, že proces profilování ve smyslu nařízení nemusí být zcela automatizovaný, ale že může být zapojen i lidský faktor.

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.

Nosič informací

Nebo také datové či paměťové médium, datový nosič či záznamové médium. Jedná se o paměťový nosič datových informací (dat) používající k jejich uchování nějaký fyzikální princip. Kromě elektronických lze za datová média považovat i jakékoli jiné hmotné nosiče, pokud slouží k zaznamenání určité informace. Dalším typem je tištěná informace.

Informace
Údaj (data) v listinné či elektronické podobě, kterému je přiřazen význam a který obsahuje osobní údaj.

Dokument
Každá písemná, obrazová, zvuková nebo jinak zaznamenaná informace, ať již v podobě listinné (analogové) nebo elektronické (digitální), která byla vytvořena v rámci Organizace nebo byla Organizaci doručena.

Zveřejněný osobní údaj
Osobní údaj zpřístupněný neurčitému okruhu příjemců zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.

Evidence/katalog
Soubor informací, jehož obecným znakem je způsob, jakým jsou informace o osobních údajích uspořádány a způsob jejich zpřístupnění.

Zvláštní právní předpis
Pro účely této směrnice se jím rozumí každý zákon, nebo právní předpis EU, který stanoví povinnost zpracování osobních údajů pro naplnění účelu daného zákona či právního předpisu EU.

2.2. Předpisy a nařízení

Směrnice se vydává v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Směrnice upravuje povinnosti Organizace a jejich zaměstnanců při provádění automatizovaného zpracování osobních údajů a při provádění neautomatizovaného zpracování těch osobních údajů, které jsou Organizací zpracovávány. Směrnice se nevztahuje na nahodilé, neúmyslné získání osobních údajů, pokud tyto údaje nejsou dále zpracovávány.

2.3. Správce osobních údajů

Organizace je v postavení Správce osobních údajů a z tohoto důvodu je zodpovědná za zpracování získávaných údajů v souladu s platnou legislativou. Organizace se zavazuje shromažďovat a vést pouze takové osobní údaje o subjektech, které umožňují poskytovat bezpečné, odborné a kvalitní služby. Pro práci s těmito osobními údaji byl vytvořen příslušný systém práce pro všechny personální úrovně, byl definován soubor osobních údajů, jejichž získávání je pro zajištění poskytování kvalitních, odborných a bezpečných služeb klientům nezbytné, dále bylo přesně vymezeno, k jakému účelu budou konkrétní osobní údaje využívány a také byla posouzena možná rizika spojená se zajištěním bezpečnosti osobních údajů a jejich správou. V kompetenčním, podpisovém řádu a pracovním řádu byly ustanoveny role/pozice odpovědné za dodržování legislativních podmínek v oblasti ochrany osobních údajů.

Dalšími právními normami upravujícími ve své příslušné části oblast rozsahu a struktury získávaných dat (především o zaměstnancích) je Zákoník práce, zákon č. 133/00 Sb., o evidenci obyvatel a další zákonné normy.

2.4. Zásady zpracování osobních údajů

Osobní údaje jsou zpracovávány v souladu s následujícími zásadami:

1) zásada zákonnosti, korektnosti a transparentnosti – osobní údaje jsou zpracovávány korektně, zákonným a transparentním způsobem,
2) zásada účelového omezení – osobní údaje jsou shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný,
3) zásada minimalizace údajů – zpracování osobních údajů je přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány,
4) zásada přesnosti – zpracovávané osobní údaje jsou přesné a v případě potřeby aktualizované, osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, musí být bezodkladně zlikvidovány nebo opraveny,
5) zásada omezení uložení – osobní údaje jsou uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány,
6) zásada integrity a důvěrnosti – osobní údaje jsou 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.

Předpokladem pro zákonné zpracování údajů o subjektech je splnění právního důvodu, tedy zpracování osobních údajů na základě:

1) splnění požadavků legislativy,
2) dodržení smluvních závazků,
3) uděleného Souhlasu od subjektu,
4) oprávněného zájmu Organizace.

2.5. Pravidla pro zpracování Souhlasu subjektu údajů

Pravidla pro zpracování Souhlasu subjektu údajů

1) Souhlas musí být svobodným, konkrétním (pro konkrétní účel zpracování), informovaným a jednoznačným projevem vůle subjektu údajů, který jím dává své svolení ke zpracování svých osobních údajů.
2) Subjekt údajů musí být před udělením souhlasu informován o všech skutečnostech zpracování, zejména o Organizaci jako správci, účelech zpracování, o operacích zpracování a o možnosti kdykoli odvolat souhlas, nikoli však se zpětnými účinky.
3) Souhlas musí být udělen v písemné formě, a to buď v listinné, nebo v elektronické podobě.
4) Pokud je od Subjektu údajů nutné získat Souhlas se zpracováním, musí se tak stát za pomoci samostatného dokumentu (v listinné nebo elektronické podobě).
5) Subjekt údajů je oprávněn jím udělený souhlas kdykoli odvolat. Odvolat souhlas musí být stejně snadné jako jej poskytnout. V případě, že Organizaci bude doručeno odvolání souhlasu je Organizace povinna postupovat v souladu s postupy uvedenými v této směrnici.
6) V případě, že subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování, Organizace je povinna provést likvidaci osobních údajů, které se daného subjektu údajů týkají.
7) Organizace eviduje informace o uděleném souhlasu v následujícím rozsahu: kdo a kdy souhlas udělil, rozsah informací poskytnutých subjektu údajů před udělením souhlasu a forma udělení souhlasu. Součástí evidence je též žádost o vyjádření souhlasu, pokud byla předložena subjektu údajů, a záznam o uděleném souhlasu. V

případě, že subjekt údajů souhlas odvolal, je součástí evidence též údaj o odvolání souhlasu a o datu odvolání souhlasu.

8) Udělený souhlas je platný pouze pro operace zpracování, které jsou nezbytné a přiměřené k naplnění účelu, pro který byl souhlas udělen.

Podmínky použitelné na souhlas dítěte

Souhlas se zpracováním osobních údajů dítěte mladšího 16ti let je platný pouze v případě, že je vyjádřen nebo schválen jeho zákonným zástupcem.

2.6. Zpracování osobních údajů

2.6.1. Oprávněný zájem organizace/správce

1) Organizace je oprávněna zpracovávat osobní údaje subjektu údajů v případě, je-li zpracování nezbytné pro účely plnění oprávněných zájmů Organizace či třetí osoby.
2) Oprávněným zájem Organizace může být např. zveřejňování osobních údajů v rámci práva na informace, přímý marketing a profilování, ochrana před zneužitím služeb, ochrana majetkových zájmů, zajištění bezpečnosti sítě a informací a z dalších důvodů.
3) V každém jednotlivém případě, kdy má dojít ke zpracování osobních údajů na základě oprávněného zájmu, je nutné stanovit oprávněný zájem a dále posoudit:
    a) oprávněnost stanoveného zájmu, tedy zda je stanovený zájem legální a dostatečně specifický a zda jde o skutečný zájem Organizace,
    b) nezbytnost zamýšleného zpracování osobních údajů pro účely stanoveného zájmu, zda je v rovnováze oprávněný zájem Organizace a práva subjektu údajů,
    c) zda nad stanoveným zájmem Organizace nepřevažují zájmy nebo základní práva a svobody subjektu údajů, včetně posouzení případného přijetí záruk k ochraně práv a svobod subjektů údajů.
4) V případě, že jsou splněny všechny výše uvedené požadavky, smí být v rámci Organizace zahájeno zpracování osobních údajů z důvodu oprávněného zájmu.

Zpracování zvláštních osobních údajů

1) Organizace smí zpracovávat zvláštní osobní údaje pouze v případech, kdy jde o některý z případů vymezených ve čl. 9 odst. 2 nařízení GDPR, zejména:
    a) subjekt údajů udělil výslovný souhlas se zpracováním zvláštních osobních údajů pro jeden či více konkrétních účelů, nebo
    b) zpracování je nezbytné pro účely plnění povinností vyplývajících ze smlouvy mezi subjektem a Organizací.

2.6.2.Vymezení práv subjektů údajů a odpovídajících povinností Správce

Žádost o přístup k osobním údajům – subjekt údajů má právo získat od Organizace potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, jakým způsobem byly získány a podobně. Subjekt má právo získat přístup k těmto osobním údajům a k následujícím informacím:

a) kontaktní informace o Organizaci/Správci
b) kontaktní informace na osobu odpovědnou za ochranu dat v Organizaci či o pověřenci, je-li ustanoven

c) kompletní výčet účelů a právních důvodů zpracování včetně případných oprávněných zájmech,
d) kategorie dotčených osobních údajů,
e) o příjemci nebo kategorii příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích, pokud se osobní údaje předávají do třetí země nebo mezinárodní organizaci, má subjekt údajů právo být informován o vhodných zárukách, které se vztahují na předání,
f) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby,
g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
h) skutečnost, že zde dochází či ne k automatizovanému rozhodování, včetně profilování, a smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

V případě kladného vyřízení žádosti subjektu údajů, Organizace poskytne žadateli potvrzení, zda osobní údaje jsou, či nejsou zpracovávány a dále osobní údaje v rozsahu požadovaném subjektem údajů.

1) Žádost o opravu osobních údajů – subjekt údajů má právo na to, aby Organizace bez zbytečného odkladu opravila nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů.

Organizace je povinna ověřit, zda jsou osobní údaje, k nimž se žádost o opravu vztahuje, přesné. Po ověření správnosti údajů či jejich opravě je Organizace povinna o tomto informovat subjekt údajů.

2) Žádost o likvidaci osobních údajů – subjekt údajů má právo na to, aby Organizace bez zbytečného odkladu provedla likvidaci osobních údajů, které se daného subjektu údajů týkají. Organizace má povinnost bez zbytečného odkladu provést likvidaci osobních údajů, pokud je dán jeden z těchto důvodů:
   a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
   b) subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,
   c) subjekt údajů vznese námitky proti zpracování a neexistují žádné oprávněné důvody pro zpracování,
   d) osobní údaje byly zpracovány protiprávně,
   e) osobní údaje musí být zlikvidovány ke splnění právní povinnosti stanovené v právu EU nebo obecně závazným právním předpisem,
   f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti.
3) Shledá-li Organizace, že se na danou situaci uplatní jedna z níže uvedených výjimek a daného cíle nelze dosáhnout jiným způsobem než zpracováním osobních údajů, může odmítnout provést likvidaci osobních údajů. Zpracování osobních údajů je nezbytné:
   a) pro výkon práva na svobodu projevu a informace,
   b) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva EU nebo obecně závazného právního předpisu, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je Správce pověřen,
   c) z důvodů veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3 nařízení GDPR,

d) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1 nařízení, pokud je pravděpodobné, že by právo na likvidaci osobních údajů znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování,
e) pro určení, výkon nebo obhajobu právních nároků.

V případech, že jsou naplněny podmínky likvidace osobních údajů a organizace žádosti subjektu údajů vyhoví, je povinna na základě vlastních zaznamenaných údajů ohledně předávání osobních údajů jiným správcům, kteří tyto osobní údaje zpracovávají, tyto Správce informovat, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.

4) Žádost o omezení zpracování osobních údajů – subjekt údajů má právo na to, aby Organizace omezila zpracování osobních údajů, v kterémkoli z těchto případů:
   a) subjekt údajů uplatnil právo na opravu osobních údajů, a to na dobu potřebnou k tomu, aby Organizace mohla správnost osobních údajů ověřit,
   b) Správce zpracovával osobní údaje subjektu údajů v rozporu se zákonem a subjekt údajů nevyžaduje likvidaci osobních údajů a žádá místo toho omezení jejich zpracování,
   c) Správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků,
   d) subjekt údajů vznesl námitku proti zpracování, a to na dobu, po kterou bude Správce posuzovat, jestli námitce vyhoví, tedy zda oprávněné důvody Správce převažují nad oprávněnými důvody subjektu údajů.

V případě, že Organizace posoudí, že je naplněna alespoň jedna z podmínek, označí uložené osobní údaje za účelem omezení jejich dalšího zpracování. Organizace je oprávněna takto označené osobní údaje zpracovávat, s výjimkou jejich uložení, 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 České republiky.
Organizace omezení zpracování osobních údajů neprodleně zruší a subjekt údajů předem o tomto zrušení informuje, pokud pomine důvod omezení zpracování.

5) Žádost o získání a přenesení osobních údajů – subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl Organizaci, ve strukturovaném, běžně používaném a strojově čitelném formátu, v případě, že se zpracování osobních údajů provádí automatizovaně a zároveň je založeno na:
   a) souhlasu subjektu údajů nebo
   b) smlouvě, jejíž smluvní stranou je subjekt údajů.

6) Námitka proti zpracování osobních údajů – subjekt údajů má právo kdykoliv vnést námitku proti zpracování osobních údajů.
7) Stížnost na postup Správce – subjekt údajů má právo se obrátit se stížností na vedení Organizace případně Pověřence (je-li ustanoven), pokud se domnívá, že Organizace zpracováním jeho osobních údajů porušuje nařízení nebo není-li spokojen s postupem Organizace při vyřizování jeho žádosti za účelem výkonu jeho práv. Vedení musí na podněty reagovat nejpozději do 30 dnů.
8) Podání stížnosti u Úřadu – subjekt údajů má právo podat stížnost u úřadu, pokud se domnívá, že Organizace zpracováním jeho osobních údajů porušuje nařízení. (Podáním stížnosti není vyloučena možnost využít jiné prostředky správní nebo soudní ochrany).

2.6.3. Postupy Správce při výkonu práv subjektů údajů

1) Subjekt údajů za účelem výkonu svých práv může podat žádost osobně, písemně či v elektronické formě (prostřednictvím datové schránky, zveřejněné e-mailové schránky).
2) Organizace předá informaci či jinak vyřídí žádost subjektu údajů ve formě preferované subjektem údajů. Pokud ji subjekt údajů nezvolil, platí, že odpověď a další komunikace probíhá ve formě odpovídající podané žádosti. V případě, že subjekt údajů podal žádost v elektronické formě, Organizace poskytne informace v elektronické formě, je-li to možné, pokud subjekt údajů nepožádá o jiný způsob.
3) Po převzetí žádosti odpovědná osoba v Organizaci (definovaná v organizační struktuře organizace či dle pracovní pozice jako osoba odpovědná za oblast bezpečnosti ochrany osobních údajů, pokud tomu tak není pak samotné vedení Organizace) žádost zaeviduje a zahájí její vyřízení.
4) Organizace je jako Správce povinna ověřit totožnost žadatele a určit, zda se skutečně jedná o oprávněný subjekt údajů. Pokud žádost neobsahuje dostatek údajů k tomu, aby Organizace mohla žadatele či subjekt údajů bezpečně identifikovat, vyzve žadatele, aby svou žádost doplnil dodatečnými informacemi nezbytnými k potvrzení totožnosti subjektu údajů a případnými informacemi o službách, které využívá. V případě, že ani po tomto doplnění nebude možné subjekt údajů identifikovat, pak Organizace informuje o této skutečnosti žadatele a výkon práva neumožní.
5) Organizace je povinna podle náležitostí přijaté žádosti bez zbytečného odkladu, a vždy do jednoho měsíce od obdržení žádosti poskytnout žadateli/subjektu údajů informace o přijatých krocích. Lhůtu jednoho měsíce je možné o další dva měsíce prodloužit s ohledem na složitost a počet žádostí přijatých během období jednoho měsíce od přijetí žádosti. V prodloužené lhůtě nelze žádost odmítnout. Organizace musí informovat žadatele/ subjekt údajů o jakémkoliv takovém prodloužení do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad.
6) Pokud Organizace žádost odmítne, bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti informuje žadatele/subjekt údajů o důvodech odmítnutí a o možnosti podat stížnost u úřadu a žádat o soudní ochranu.
7) Organizace poskytuje informace v rámci výkonu práv subjektu údajů bezplatně.
8) V případě, že Organizace žádost vyhodnotí jako zjevně nedůvodnou nebo nepřiměřenou, má právo žádost odmítnout nebo vyřízení žádosti zpoplatnit. Organizace před vyměřením přiměřeného poplatku informuje žadatele o jeho výši a požádá jej o souhlas.
9) Organizace je povinna oznámit jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy, likvidaci osobních údajů nebo omezení zpracování s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí.

Pověřenec pro ochranu osobních údajů – je-li ustanoven

Organizace po provedené analýze dat, zjistila, že nemá povinnost ustanovit pověřence pro ochranu osobních údajů.

2.6.4. Odpovědnost a povinnosti Správce při zpracování osobních údajů

1) Organizace jako Správce odpovídá za dodržování jednotlivých povinností stanovených právními předpisy upravujícími ochranu osobních údajů.
2) Organizace má definované role a odpovědnosti při zpracování osobních údajů v rámci své působnosti (ustanovené v organizačním/pracovním řádem a pracovními náplněmi).

3) Organizace vystupuje převážně v roli Správce.
4) Zmocnění ke zpracování osobních údajů vyplývá ze zvláštního právního předpisu nebo ze smlouvy o zpracování osobních údajů, případně z uděleného Souhlasu od subjektu. Ve všech případech musí být dostatečným způsobem upraveny požadavky na vhodná technická a organizační opatření na ochranu osobních údajů.
5) Pokud se na zpracování osobních údajů v gesci Správce podílí třetí strana (Zpracovatel), pak Organizace smí využít pouze takového Zpracovatele, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky stanovené nařízením a touto směrnicí a aby byla zajištěna ochrana práv subjektů. Smlouva o zpracování osobních údajů Zpracovatelem musí mít písemnou formu. Ve smlouvě musí být uveden předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva Správce, požadavky na vhodná technická a organizační opatření na ochranu osobních údajů, resp. záruky Zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů, jež má dle smlouvy zpracovat, a požadavky na poskytování součinnosti při ohlašování případů porušení zabezpečení osobních údajů úřadu. Smlouva musí obsahovat i další náležitosti stanovené v čl. 28 odst. 3 nařízení.
6) Organizace v pozici Správce určuje účely a prostředky zpracování osobních údajů a nese za tuto činnost odpovědnost. Jestliže Organizace zjistí, že Zpracovatel porušuje povinnosti stanovené nařízením, je povinna na tuto skutečnost Zpracovatele neprodleně upozornit a ukončit zpracování osobních údajů Zpracovatelem.
7) Organizace jako Správce nebo Zpracovatel spolupracuje na požádání s úřadem při plnění jeho úkolů

Záznamy o činnostech zpracování (u organizací nad 250 zaměstnanců, případně v případě vysokého rizika pro ochranu osobních údajů)

Organizace nemá 250 zaměstnanců.

2.6.5. Zpracování osobních údajů v rámci Organizace

V rámci Organizace je povoleno zpracovávat osobní údaje pouze za podmínek stanovených nařízením a touto směrnicí.

1) Řízení lidských zdrojů - V rámci lidských zdrojů je možné zpracovávat osobní údaje o zaměstnancích stanovené zvláštními zákony (např. zákonem č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, zákonem č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů, zákonem č. 48/1997 Sb., o veřejném zdravotním pojištění, ve znění pozdějších předpisů, apod.), a to pro účely pracovněprávního vztahu a pro plnění úkolů uložených zákonem č. 262/2006 Sb., zákoníkem práce, ve znění pozdějších předpisů, nebo zvláštním právním předpisem, po dobu nezbytnou k zajištění práv a povinností, plynoucích z tohoto pracovněprávního nebo jiného obdobného vztahu.
   Formuláře používané v rámci řízení lidských zdrojů týkající se ochrany osobních údajů jsou připravovány a průběžně aktualizovány. Mimo listinou formu jsou zpracovávány v systému Helios.
2) Evidence návštěv při vstupu osob, které nejsou v pracovněprávním vztahu nebo v jiném obdobném vztahu k Organizaci, do jejích prostor, jež nejsou určeny pro veřejnost, je požadováno jméno a příjmení, druh a číslo dokladu totožnosti.

Uvedené údaje jsou zpracovávány pro účely oprávněných zájmů Organizace. Mohou být zpracovány bez souhlasu subjektu údajů.

3) Kontaktní údaje osob ze smluv

Zabezpečení zpracování osobních údajů

Organizace je jako Správce osobních údajů při zabezpečení osobních údajů povinna:

1) posuzovat rizika, která při zpracování osobních údajů hrozí a přijmout taková technická a organizační opatření, aby nemohlo dojít k nahodilému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů,
2) provést taková technická a organizační opatření, aby úroveň zabezpečení odpovídala danému riziku v souladu s nařízením,
3) zpracovat a evidovat přijatá a provedená technická a organizační opatření k zajištění ochrany osobních údajů v souladu s nařízením a zvláštními a interními předpisy,
4) zajistit, že užívat systémy pro automatizované zpracování osobních údajů mohou pouze oprávněné osoby, a to pouze v rozsahu odpovídajícímu jejich oprávnění,
5) zajistit elektronické záznamy o přístupu k osobním údajům a provedených úkonech i zpracování osobních údajů,
6) zabránit neoprávněnému přístupu k nosičům informací,
7) posoudit, zda bude docházet k předání osobních údajů třetím osobám a zda jsou splněny všechny podmínky předání v souladu s nařízením a touto směrnicí.

3 Evidence přijatých organizačních a technických opatření

3.1. Organizační a technická opatření

1) Personální bezpečnost

S osobními údaji je oprávněna se seznámit pouze oprávněná osoba, a to v rozsahu odpovídajícímu jejímu oprávnění. Oprávnění této osoby vyplývá z její pracovní náplně na základě uzavřeného pracovněprávního vztahu nebo obdobného vztahu. Oprávněná osoba musí mít objektivní a důvodnou potřebu seznámit se s osobními údaji za účelem plnění pracovních povinností či jiných povinností nebo oprávněných zájmů.

2) Fyzická bezpečnost

Dokumenty s osobními údaji se ukládají na příslušných pracovištích (kanceláře, archivy apod.) v souladu se Spisovým řádem a ostatními interními předpisy.

Dokumenty musí být ukládány v uzamčených schránkách (kancelářské skříně, trezorové skříně, plechové skříně, stolní kontejnery apod.), bez možnosti přístupu neoprávněných osob v mimopracovní době i v době krátkodobé nepřítomnosti (oběd, přestávka apod.).

Klíč od uzamčené schránky disponuje vlastník procesů nebo jím určená osoba. Duplikáty klíčů od uzamčené schránky jsou uloženy u přímého nadřízeného vlastníka procesů nebo jím určené osoby v zapečetěné obálce.

V době nepřítomnosti vlastníka procesu může uzamčenou schránku bez souhlasu vlastníka procesu otevřít pouze nejblíže nadřízený zaměstnanec vlastníka procesu nebo jím určená osoba.

Při skončení pracovněprávního vztahu vlastníka procesu zabezpečí předání údajů jiné osobě nejblíže nadřízený zaměstnanec vlastníka procesu. Pokud není přebírající znám, vlastník informace předá dokumenty nejblíže nadřízenému zaměstnanci, nebo dokumenty uloží do spisovny Organizace v zabezpečeném obalu, ke kterému přiloží seznam ukládaných dokumentů.

3) Informační bezpečnost osobních údajů ukládaných v ICT Organizace

Zabezpečení přístupu k osobním údajům zpracovávaných v ICT Organizace vychází ze směrnic uvedených v připojené tabulce, které jsou v souladu s doporučením řady norem ISO/IEC 27000.

Osobní údaje nesmí být zasílány mimo datovou síť Organizace a pokud možno ani v rámci datové sítě Organizace v nezašifrované podobě.

4) Likvidace osobních údajů

Organizace je povinna provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány nebo na základě žádosti subjektu údajů.

Při skartaci dokumentů obsahující osobní údaje je třeba dbát bezpečnostních opatření.

Dokumenty obsahující osobní údaje v listinné podobě určené k likvidaci se sepíší do skartačního seznamu, zařadí do skartačního řízení a po odsouhlasení skartačního návrhu se předají k fyzické likvidaci.

Dokumenty musí být likvidovány v souladu s interním předpisem Spisový a skartační řád.

3. 2. Ohlašování případů porušení zabezpečení osobních údajů úřadu

1) Zaměstnanec Organizace je povinen ohlásit nadřízenému jakoukoliv skutečnost zakládající potenciální porušení zabezpečení osobních údajů bez zbytečného odkladu od okamžiku, kdy skutečnost zakládající potenciální porušení zjistil.
2) Pověřená osoba zahájí ve spolupráci dotčenými útvary interní vyšetřování. Pokud ze závěru interního vyšetřování vyplývá, že k porušení zabezpečení osobních údajů došlo a je zde riziko pro práva a povinnosti fyzických osob, ohlásí pověřená osoba/pověřenec tuto skutečnost bez zbytečného odkladu úřadu.
3) Ohlášení musí být doručeno úřadu bez zbytečného odkladu, nejpozději do 72 hodin od zjištění skutečnosti, která s vysokou pravděpodobností představuje porušení zabezpečení osobních údajů. Pokud do této lhůty není ohlášení úřadu doručeno, musí být zároveň s ohlášením uvedeny relevantní důvody tohoto zpoždění.
4) Ohlášení dle odst. musí mít písemnou formu a musí obsahovat:
   a) popis povahy daného porušení zabezpečení osobních údajů. Pokud je to možné včetně kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného počtu dotčených záznamů subjektů údajů,
   b) jméno a kontaktní údaje pověřené osoby/ pověřence,
   c) popis pravděpodobných důsledků, které porušení zabezpečení osobních údajů představuje,
   d) popis nápravných opatření, která byla přijata nebo navržena k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.
   e) Organizace oznámí bez zbytečného odkladu po ukončení interního vyšetřování dle kapitoly subjektu údajů porušení zabezpečení osobních údajů, pokud toto porušení bylo v závěru interního vyšetřování vyhodnoceno jako vysoce rizikové pro práva a povinnosti fyzických osob.
   f) Oznámení není nutné činit v případě, že:
      - byla zavedena náležitá technická a organizační opatření a tato byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup (např. šifrování),

- byla přijata nápravná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektu údajů se již pravděpodobně neprojeví,
- by to vyžadovalo nepřiměřené úsilí. V takovém případě musí být subjekt údajů informován stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Posouzení vlivu na ochranu osobních údajů

Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, Organizace je povinna před zpracováním osobních údajů provést posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Následně, pokud rizika budou vysoká a neošetřitelná, pak přistoupit ke konzultaci s úřadem.

související dokumenty

INTERNÍ	
P-01	Příručka kvality
Řád - 2	Kompetenční a podpisový řád
Řád - 3	Pracovní řád
SM - 00	Řízení dokumentace
SM - 01	Personalistika, mzdy
SM - 13	Spisová služba
	Nová dokumentace IT MONTPROJEKT, a.s.
	Katalog EPI
	Evidence a analýzy rizik MONTPROJEKT, a.s.
	DPO – analýza povinnosti stanovit pověřence MONTPROJEKT, a.s.
	Rizika V1
	Dodatek ke smlouvám - mlčenlivost
	Souhlas s OOU
	Informace o zpracování OU zaměstnanci
EXTERNÍ	
Nařízení Evropského parlamentu a Rady č. 2016/679	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně

	osobních údajů)
Zákon č. 89/2012 Sb.	občanský zákoník, ve znění pozdějších předpisů

Příloha 1:

Stanovení oprávnění a přehled osob, které mají právo přístupu k osobním údajům v Organizaci

	Stanovení oprávnění a přehled osob, které oprávněním přístupu k citlivým osobním údajům v Organizaci disponují	Smlouvy	zaměstnancůOsobní údaje	OrganizaceDalší evidence
1.	Ředitel	☺	☺	
2.	Ekonom		☺	☺
3.	Účetní			☺
4.	Personalista, mzdová účetní		☺	

Příloha 2: Přehled o zpracovávání údajů

katalog OU.xlsx

1

4 ZÁVĚREČNÁ USTANOVENÍ

4.1 Účinnost směrnice

Tato směrnice nabývá účinnosti dne 30. 4. 2018.

4.2 Zrušovací ustanovení

Touto směrnicí se neruší žádná směrnice.

4.3 Návazné ŘA

P – 01 Příručka kvality
Ř – 02 Kompetenční a podpisový řád
Ř – 03 Pracovní řád
SM – 00 Řízení dokumentace
SM – 13 Spisová služba
SM – 01 Personální směrnice

4.4 Zaváděná dokumentace

Katalog EPI