Směrnice upravující zpracování a ochranu osobních údajů ve společnosti __(Centrum pro rodinu Kyjov, o.p.s.)__

Obsah

Úvodní ustanovení

Článek I.
Důvody úpravy

1.1 V souvislosti s nabytím účinnosti nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“) přijímá společnost Centrum pro rodinu Kyjov, o.p.s., IČ 293 76 556, se sídlem Palackého tř. 64/1, Kyjov 697 01 (dále jen „společnost“ nebo „organizace“) tuto Směrnici upravující zpracování a ochranu osobních údajů (dále jen „Směrnice“).

Článek II.
Předmět úpravy a rozsah působnosti

2.1 Směrnice upravuje postupy zpracování a ochrany osobních údajů zpracovávaných společností v rámci její činnosti jako správce a zpracovatele a povinnosti zaměstnanců a dalších osob v obdobném právním vztahu ke společnosti jako zaměstnanci podílející se na zpracování osobních údajů společností.

2.2 Směrnice se vztahuje na veškeré činnosti zpracování osobních údajů prováděné společností v postavení správce i zpracovatele a na všechny zaměstnance a osoby v obdobném právním vztahu ke společnosti jako zaměstnanci.

2.3 V případě, že jiný předpis práva světského stanoví přísnější pravidla než Směrnice, použije se takového předpisu.

2.4 V případě, že jiné vnitřní předpisy stanoví mírnější pravidla pro zpracování osobních údajů, má Směrnice před těmito předpisy aplikační přednost.

Článek III.
Definice pojmů

3.1 Není-li dále stanoveno jinak, mají následující pojmy pro účely směrnice tento význam:

a) osobním údajem se rozumí jakákoli informace o identifikované nebo identifikovatelné osobě; identifikovatelnou osobou je každá osoba, kterou lze identifikovat na základě konkrétního osobního údaje buď přímo, nebo ve spojení s jiným osobním údajem;

b) citlivými osobními údaji se rozumí osobní údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické údaje, biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu či sexuálním životě nebo sexuální orientaci fyzické osoby a údaje o trestných činech a rozsudcích v trestních věcech;

c) důvěrnými osobními údaji se rozumí takové osobní údaje, které fyzické osoby, kterých se týkají, považují za zvlášť významné pro svá práva a svobody;

d) subjektem údajů se rozumí fyzická osoba, které se osobní údaje týkají; subjektem údajů není zesnulá fyzická osoba;

e) zaměstnanci se rozumí osoby v pracovním poměru ke společnosti, osoby vykonávající pro společnost závislou práci na základě dohody o provedení práce nebo dohody o pracovní činnosti, a jiné osoby v obdobném právním vztahu ke společnosti jako osoby v pracovním poměru.

f) zpracováním osobních údajů se rozumí jakákoli operace nebo soubor operací prováděné s osobními údaji nebo jejich souborem, zejména jejich 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;
g) činností zpracování se rozumí soubor operací zpracování osobních údajů prováděných za jedním účelem;
h) správcem osobních údajů se rozumí osoba určující způsob a účel zpracování osobních údajů; zpracování osobních údajů prováděné zaměstnanci správce podle jeho pokynů se počítá jako zpracování osobních údajů prováděné správcem;
i) zpracovatelem osobních údajů se rozumí osoba odlišná od zaměstnance, která pro správce provádí zpracování osobních údajů;
j) odpovědným zaměstnancem se rozumí zaměstnanec dohlížející na dodržování právních předpisů a vnitřních předpisů společnosti u konkrétní činnosti zpracování a zodpovídající za jejich dodržování.

Základní povinnosti

Článek IV.
Zásady zpracování

4.1 Společnost provádí zpracování osobních údajů pouze na základě zákonného titulu pro zpracování ve smyslu čl. 6 GDPR a pouze pro účely, pro které byly osobní údaje shromážděny. Pro jiný účel mohou být osobní údaje zpracovávány pouze na základě souhlasu subjektu údajů, zákonné povinnosti stanovené právem České republiky nebo Evropské unie, nebo pokud jsou naplněny podmínky podle čl. 6 odst. 4 GDPR.
4.2 Zpracování osobních údajů je přípustné pouze za dodržení zásad zákonného zpracování ve smyslu čl. 5 GDPR. Společnost dbá o spravedlivé a transparentní zacházení se subjekty údajů a jejich osobními údaji a o dodržování práv subjektů údajů.
4.3 Osobní údaje mohou být shromažďovány a zpracovávány pouze pro konkrétně stanovený účel a pouze v rozsahu a způsobem, který je nezbytný pro dosažení stanoveného účelu.
4.4 Osobní údaje nejsou zpracovávány po dobu delší, než je nezbytně nutné. Doba uchování jednotlivých druhů dokumentů obsahujících osobní údaje se řídí platnými právními předpisy České republiky a Evropské unie, spisovým a skartačním řádem společnosti a dalšími vnitřními předpisy společnosti.
4.5 Pokud jsou osobní údaje zpracovávány na základě souhlasu subjektu údajů, dbají zaměstnanci o to, aby byl udělený souhlas svobodný a informovaný. Zakazuje se uvádět souhlasy se zpracováním osobních údajů do smluv, obchodních podmínek a jiných dokumentů, v jejichž rámci by neudělení souhlasu mělo negativní následky pro subjekt údajů.
4.6 V případě zjištění, že zpracování osobních údajů společností nesplňuje v některém případě některou ze zásad, bude zpracování osobních údajů až do vyřešení nedostatku omezeno. Nelze-li nedostatek odstranit, bude zpracování ukončeno.
4.7 Společnost dbá při zpracování osobních údajů na dodržování svých povinností v oblasti zabezpečení osobních údajů ve smyslu čl. 24, 25 a 32 GDPR a dalších ustanovení ukládajících společnosti povinnosti jako správci nebo zpracovateli osobních údajů.
4.8 Při zavádění opatření k ochraně osobních údajů je dbáno na to, aby byla opatření přiměřená povaze zpracování osobních údajů, kategorii a množství zpracovávaných osobních údajů a míře rizika, které při zpracování osobních údajů hrozí, a to jak z pohledu pravděpodobnosti vzniku újmy pro subjekty údajů, tak její potenciální výši.

Článek V.
Pověření zaměstnanců

5.1 Společnost po provedení potřebných analýz dospěla k závěru, že rozsah jí zpracovávaných osobních údajů nevyžaduje jmenovat pověřence pro ochranu osobních údajů. Přesto pro koordinaci ochrany osobních údajů v organizaci jmenuje společnost interního zaměstnance jako koordinátora GDPR. Úkoly koordinátora GDPR jsou:

a) zajišťovat jednotnost procesů zpracování osobních údajů společností v rámci celé její organizační struktury,
b) sjednocovat postupy odpovědných zaměstnanců,
c) přijímat a vyhodnocovat podněty a informace zaměstnanců ve věci ochrany osobních údajů, hrozících rizik a zkvalitnění procesů zpracování,
d) předkládat vyhodnocené podněty a informace podle písm. b) s doporučeními jednateli společnosti,
e) koordinovat zavádění nových procesů a opatření týkajících se zpracování osobních údajů ve společnosti do praxe,
f) vyhodnocovat připomínky k analýze rizik v rámci zavádění záměrné a standardní ochrany osobních údajů.
g) vést evidenci záznamů o činnostech zpracování, seznamů zaměstnanců, vnitřních předpisů týkajících se ochrany osobních údajů, analýz rizik a dalších dokumentů vypracovávaných podle Směrnice nebo GDPR v souvislosti s ochranou osobních údajů,
h) sloužit jako kontaktní místo pro subjekty údajů ve věcech souvisejících se zpracováním jejich osobních údajů,
i) koordinovat vyřizování žádostí subjektů údajů o uplatnění jejich práv,
j) vést evidenci žádostí subjektů údajů o uplatnění práv a reakcí na ně.

5.2 Pro každou činnost zpracování je určen odpovědný zaměstnanec. Při minimálním počtu činností zpracování může být odpovědným zaměstnancem koordinátor GDPR. Úkoly odpovědného zaměstnance jsou:

a) dohlížet na dodržování GDPR a tohoto předpisu v rámci jim svěřených činností zpracování,
b) ukládat zaměstnancům úkoly související s jim svěřenou činností zpracování,
c) vypracovávat posouzení vlivu činnosti na ochranu osobních údajů,
d) vypracovávat analýzu rizik v rámci zavádění záměrné a standardní ochrany osobních údajů,
e) spolupracovat s koordinátorem GDPR na řešení incidentů porušení zabezpečení, zlepšování úrovně ochrany osobních údajů a zavádění nových procesů a na vyřizování žádostí subjektů údajů o uplatnění práv.

5.3 Koordinátor GDPR, vedoucí zaměstnanci a odpovědní zaměstnanci jsou povinni absolvovat jednou ročně školení týkající se otázek informační bezpečnosti a ochrany osobních údajů.

Článek VI.
Povinnosti zaměstnanců

6.1 Zaměstnancům je zakázáno provádět jménem společnosti jakékoli zpracování osobních údajů, které jim nebylo společností přímo uloženo v rámci jejich pracovního nebo obdobného poměru. Zaměstnanci zpracovávají osobní údaje výhradně způsobem a v rozsahu stanoveném společností.

6.2 Zaměstnancům je zakázáno předávat osobní údaje zpracovávané společností třetím osobám, pokud jim to neukládá právní předpis České republiky nebo Evropské unie nebo jim to nevyplývá z jejich pracovní náplně nebo jim to není společností přímo uloženo.

6.3 Zaměstnanci jsou povinni zachovávat mlčenlivost o všech skutečnostech, o kterých se v rámci zpracování osobních údajů dozvědí, a to i po skončení pracovního poměru. Tím nejsou dotčeny jejich povinnosti vyplývající z jiných právních předpisů.
6.4 V rámci zpracování osobních údajů dbají zaměstnanci na to, aby k dokumentům obsahujícím osobní údaje neměly přístup neoprávněné osoby, ať již zaměstnanci společnosti nebo jiné osoby.
6.5 Zaměstnanci jsou povinni dodržovat vnitřní předpisy společnosti dotýkající se ochrany osobních údajů, zejména tuto směrnici, spisový a skartační řád a předpisy o využívání informačních systémů a IT oblasti jako takové.
6.6 V rámci zpracování osobních údajů, které je jim společností uloženo, zaměstnanci průběžně kontrolují, zda jsou zpracovávané osobní údaje přesné, zda jsou pro daný účel potřebné a zda pro dosažení účelu zpracování není potřeba zpracovávat další osobní údaje. V případě zjištění nepřesnosti osobních údajů jsou zaměstnanci povinni vyvinout úsilí k nápravě tohoto stavu. V případě, že jsou zpracovávané osobní údaje nadbytečné nebo jsou potřebné další osobní údaje, vyrozumí o tom zaměstnanci odpovědného zaměstnance.
6.7 Zaměstnanci jsou povinni seznámit se s příslušnými ustanoveními GDPR a řídit se jimi. Porušení této povinnosti může být posouzeno jako nesplnění požadavků pro řádný výkon práce ve smyslu zákona č. 262/2006 Sb., zákoník práce.
6.8 Zaměstnanci absolvují jednou za dva roky povinné školení o informační bezpečnosti a ochraně osobních údajů.
6.9 Nově přijatí zaměstnanci, kteří se mají podílet na zpracování osobních údajů společností absolvují povinné školení o informační bezpečnosti a ochraně osobních údajů nejpozději do 2 měsíců od jejich nástupu. Za absolvování školení o informační bezpečnosti a ochraně osobních údajů se považuje také účast na pravidelném školení uvedeném v bodě 6.8 Směrnice za předpokladu, že toto školení se koná ne později než jeden měsíc od uplynutí lhůty uvedené v předchozí větě.

Článek VII.
Koordinátor GDPR

7.1 Společnost jmenuje Koordinátora GDPR.
7.2 Koordinátor GDPR může být zaměstnanec společnosti nebo osoba plnící funkci koordinátora základě jiného právního vztahu („externí osoba“).
7.3 Koordinátor GDPR plní následující úkoly:
   a) poskytuje poradenství společnosti a zaměstnancům v otázkách souvisejících se zpracováním osobních údajů nebo zajišťuje konzultaci problematiky u odborníků,
   b) přijímá podněty zaměstnanců ve věcech souvisejících s ochranou osobních údajů,
   c) dohlíží na dodržování právních předpisů České republiky a Evropské unie týkajících se zpracování osobních údajů a této směrnice,
   d) vypracovává stanovisko k posouzení vlivu činnosti na ochranu osobních údajů,
   e) spolupracuje s Úřadem pro ochranu osobních údajů a slouží jako jeho kontaktní místo,
   f) spolupracuje při vyřizování žádostí subjektů údajů o uplatnění jejich práv,
   g) jednou ročně vypracovává soubornou zprávu o stavu ochrany osobních údajů ve společnosti pro potřeby společnosti.
7.4 Koordinátor GDPR přijímá pokyny týkající se způsobu plnění jeho úkolů a ze své činnosti se zodpovídá statutárnímu orgánu společnosti.
7.5 Statutární orgán společnosti projednává soubornou zprávu podle bodu 7.4 písm. g) s vedoucími jednotlivých oddělení organizace a ve spolupráci s nimi stanovuje kroky k odstranění nedostatků a ke zlepšení praxe zpracování osobních údajů ve společnosti.
7.6 Koordinátor GDPR je oprávněn při zjištění závažného pochybení při zpracování osobních údajů spočívajícího v chybném nastavení procesů nebo bezpečnostních opatření přikázat zaměstnancům pozastavit zpracování osobních údajů. V takovém případě okamžitě informuje

vedoucího zaměstnance oddělení, v jehož rámci ke zpracování osobních údajů dochází, a statutární orgán společnosti. Do vyřešení zjištěného problému nemůže být rozhodnuto o obnovení zpracování osobních údajů.

7.7 Zaměstnanci jsou povinni poskytnout koordinátorovi GDPR maximální součinnost při plnění jeho úkolů a řídí se jeho pokyny při vyřizování žádostí subjektů údajů a při omezení zpracování podle bodu 7.7 Směrnice.

Článek VIII.
Externí zpracovatelé

8.1 Je-li nezbytné využít při zpracování osobních údajů služeb externího zpracovatele, uzavře společnost s externím zpracovatelem smlouvu o zpracování osobních údajů. Smlouva specifikuje činnost zpracovatele pro společnost a obsahuje náležitosti podle čl. 28 GDPR.

8.2 Společnost dbá při výběru zpracovatele na jeho důvěryhodnost a požaduje záruky, že bude dodržovat všechna ustanovení GDPR, zejména že bude dbát o ochranu osobních údajů a vyvine vůči společnosti veškerou potřebnou součinnost při řešení žádostí subjektů údajů a při řešení incidentů porušení zabezpečení.

8.3 Zpracovatel se ve smlouvě o zpracování osobních údajů zaváže k zajištění srovnatelného nebo vyššího standardu ochrany osobních údajů, jaký požaduje tato Směrnice.

Článek IX.
Posouzení vlivu činnosti zpracování na ochranu osobních údajů

9.1 V případě, že společnost rozhodne o zahájení činnosti, k jejímuž provedení je nutné provádět zpracování osobních údajů, určí osoba, která o zahájení činnosti a způsobu jejího provádění rozhodla, odpovědného zaměstnance.

9.2 Odpovědný zaměstnanec vypracuje posouzení vlivu činnosti zpracování na ochranu osobních údajů ve smyslu čl. 35 GDPR nebo na základě výjimek stanovených v GDPR určí, že posouzení není třeba vypracovávat.

9.3 Ustanovení bodu 9.1 a 9.2 platí obdobně, pokud společnost rozhodne o zavedení nové technologie v rámci stávajících činností zpracování osobních údajů.

9.4 Posouzení vlivu činnosti zpracování na ochranu osobních údajů je předáno k přezkoumání koordinátorovi GDPR, který k němu zaujme ve lhůtě 3 týdnů stanovisko a předá posouzení a stanovisko osobě, která o zahájení činnosti rozhodla, a koordinátorovi GDPR.

9.5 Osoba, která rozhodla o zahájení činnosti, dbá na doporučení koordinátora GDPR obsažená ve stanovisku podle tohoto bodu a přijme patřičná opatření. Pokud se od doporučení odchýlí, je povinna toto odchýlení podrobně zdůvodnit. O přijatých opatřeních a odůvodnění odchýlení informuje koordinátora GDPR.

9.6 Je-li na základě posouzení pravděpodobné, že činnost zpracování osobních údajů nese rizika pro práva a svobody subjektů údajů, pověří osoba, která o zahájení činnosti rozhodla, ve spolupráci se statutárním orgánem společnosti a koordinátorem GDPR, zaměstnance příslušných oddělení, aby navrhli opatření k odstranění nebo zmírnění rizik.

9.7 Není-li možné snížit rizika na přiměřenou úroveň, přehodnotí osoba, která o zahájení činnosti rozhodla, své rozhodnutí a navrhne úpravu zahajované činnosti tak, aby bylo zpracování osobních údajů omezeno.

9.8 Není-li možné postupovat podle bodu 9.7, požádá společnost ve spolupráci s koordinátorem GDPR o předchozí konzultaci Úřad pro ochranu osobních údajů.

Článek X.

Záznamy o činnosti zpracování

10.1 O každé činnosti zpracování je vypracován záznam o činnosti zpracování.
10.2 Záznam o činnosti zpracování obsahuje:
a) jméno zaměstnance, který záznam vypracoval,
b) roli zaměstnance, který záznam vypracoval,
c) datum vypracování záznamu,
d) jméno a kontaktní údaje správce,
e) jméno a kontaktní údaje zodpovědné osoby,
f) účely zpracování,
g) kategorie subjektů údajů,
h) kategorie osobních údajů,
i) kategorie příjemců osobních údajů,
j) plánované lhůty pro uchování osobních údajů (viz spisový a skartační řád společnosti),
k) obecný popis technických a organizačních opatření na ochranu osobních údajů,
l) informaci o případném předání osobních údajů do třetí země.
10.3 Záznamy vypracovává odpovědný zaměstnanec a předává je koordinátorovi.
10.4 V případě změny v činnosti zpracování vypracuje odpovědný zaměstnanec aktualizovaný záznam o činnosti zpracování, který předá osobám podle bodu 10.3. Původní záznam o činnosti zpracování je nadále uchováván. Aktualizované záznamy o činnosti zpracování jsou číslovány vzestupnou řadou.
10.5 Záznamy dle tohoto článku se uchovávají po dobu 10 let po ukončení činnosti zpracování.

Článek XI.
Seznamy zaměstnanců

11.1 Odpovědný zaměstnanec sestavuje seznam zaměstnanců, kteří se podílejí na činnosti zpracování.
11.2 Seznam obsahuje:
a) označení činnosti zpracování,
b) jméno zaměstnance,
c) zařazení zaměstnance,
d) roli zaměstnance ve smyslu článku XIII.,
e) úkoly zaměstnance v rámci činnosti zpracování.
11.3 Kopii seznamů předá odpovědný zaměstnanec koordinátorovi GDPR.

Organizační a bezpečnostní opatření

Článek XII.
Záměrná a standardní ochrana osobních údajů

12.1 Součástí zavádění nové činnosti zpracování osobních údajů nebo nové technologie zpracování je zavedení přiměřených opatření k zajištění ochrany osobních údajů v rámci jednotlivých úkonů zpracování osobních údajů pro účely této činnosti.
12.2 Opatření podle bodu 12.1 zahrnují určení zaměstnanců, kteří se budou na činnosti zpracování podílet, podrobení zpracování opatřením zavedeným jako základní úroveň zabezpečení pro všechny činnosti zpracování prováděné společností a zavedení nových opatření pro zamezení rizikům souvisejícím s konkrétní zaváděnou činností zpracování.

12.3 Pro stanovení rizik podle bodu 12.2 vypracuje odpovědný zaměstnanec analýzu rizik. Analýza rizik se provádí v případě, že nebylo provedeno posouzení vlivu činnosti na ochranu osobních údajů podle čl. IX.

12.4 Analýza rizik obsahuje přinejmenším:

a) popis jednotlivých úkonů zpracování v rámci činnosti zpracování,
b) hrozby pro ochranu osobních údajů při jednotlivých úkonech zpracování,
c) posouzení pravděpodobnosti nastání jednotlivých hrozeb,
d) posouzení míry újmy plynoucí z jednotlivých hrozeb,
e) stanovení míry rizika plynoucího z jednotlivých hrozeb,
f) návrh opatření k odstranění nebo snížení hrozeb.

12.5 Pravděpodobnost nastání hrozby a míra újmy z hrozby plynoucí se hodnotí na stupnici 1-5. Stupeň pět představuje nejvyšší stupeň pravděpodobnosti nastání hrozby a míry újmy. Míra rizika se stanoví jako součin těchto dvou hodnot.

12.6 Odpovědný zaměstnanec předává analýzu rizik k vyjádření koordinátorovi GDPR, který ji případně konzultuje s odborníky v oblasti ochrany osobních údajů.

12.7 Do okamžiku provedení analýzy rizik a zavedení všech potřebných opatření není možné započít s činností zpracování.

Článek XIII.
Přiřazení rolí

13.1 Každému zaměstnanci je na základě jeho pracovní pozice a zařazení v organizačním řádu přiřazena role (dále také „pracovní agenda“).

13.2 Role (pracovní agenda) definuje okruh dokumentů, ke kterým je zaměstnanci poskytnut přístup, a to jak v elektronické, tak ve fyzické podobě.

13.3 Role spravuje a přiřazuje vedoucí pracovník IT oddělení na základě informací poskytnutých mu personálním oddělením nebo statutárním orgánem společnosti.

13.4 Role jsou pravidelně aktualizovány s ohledem na změny v činnostech zpracování.

Článek XIV.
Obecná pravidla přístupu k osobním údajům

14.1 Přístup k dokumentům obsahujícím osobní údaje je omezen pouze na zaměstnance, kteří s nimi musejí nezbytně pracovat pro plnění svých pracovních úkolů.

14.2 Přístup k dokumentům obsahujícím osobní údaje v elektronické podobě je řízen na základě přiřazení rolí jednotlivým zaměstnancům podle článku XIII. Základní úroveň přístupu k dokumentům je nulová. Na základě přiřazení rolí jsou zaměstnancům zpřístupňovány jednotlivé druhy dokumentů.

14.3 Zaměstnanci přistupují k dokumentům v elektronické podobě na základě přihlášení se k uživatelskému účtu. Každý zaměstnanec má přiřazenou jednu identitu spojenou s uživatelským účtem, která je pokud možno totožná pro všechny informační systémy používané společností.

14.4 Není-li možné zajistit jednotnou identitu pro všechny informační systémy a aplikace ve smyslu bodu 14.3, přijme organizace technická opatření k tomu, aby bylo uživatelské jméno každého zaměstnance v jednotlivých informačních systémech a aplikacích vždy jednoznačně přiřaditelné ke konkrétnímu zaměstnanci.

14.5 Pro přihlášení se k uživatelskému účtu je zaměstnanec povinen využívat silné heslo. Silné heslo je tvořeno alespoň osmi znaky a obsahuje alespoň tři ze čtyř následujících typů znaků: velká a malá písmena, čísla, nealfabetické znaky.

14.6 Zakazuje se zapisovat přístupová hesla ve fyzické i elektronické podobě a sdělovat ho jiným zaměstnancům a externím osobám.
14.7 Veškeré případy přístupu k dokumentům obsahujícím osobní údaje v elektronické podobě jsou zaznamenávány pomocí logování. Logy obsahují mimo jiné informaci, ze kterého uživatelského účtu došlo k přístupu k dokumentu, kdy k přístupu došlo a v čem přístup spočíval.
14.8 Přístup k dokumentům obsahujícím osobní údaje ve fyzické podobě je řízen na základě rolí ve smyslu článku XIII.
14.9 V případě, že k dokumentům ve fyzické podobě chce přistoupit zaměstnanec, jehož role to neumožňuje, je zaměstnanec, který je za dokumenty zodpovědný, povinen zjistit, zda byl zaměstnanec, byť přechodně přístupem k dokumentům pověřen. V případě, že pověřen nebyl, nebude zaměstnanci přístup umožněn.
14.10 O veškerých úkonech s dokumenty, které provádí zaměstnanec, jehož role to neumožňuje, se pořizují záznamy, které tvoří součást příslušného spisu.

Článek XV.
Zóny fyzického přístupu

15.1 Každý objekt využívaný společností zcela nebo z části k administrativním účelům bude rozdělen na přístupové zóny s odstupňovaným zabezpečením a omezením přístupu.
15.2 Do veřejné zóny spadají prostory přístupné pro externí osoby bez omezení. V této zóně je zakázáno uchovávat osobní údaje s výjimkou nezbytných případů a nutném rozsahu a za předpokladu, že jsou zavedena dostatečná bezpečnostní opatření.
15.3 Vnitřní zóna zahrnuje prostory ve vnitřním objektu, ve kterých se samostatně pohybují pouze zaměstnanci. Vstup do této zóny je umožněn pouze za použití klíče nebo identifikační čipové karty. Pohyb externích osob včetně dodavatelů služeb je ve vnitřní zóně umožněn pouze v doprovodu zaměstnance.
15.4 Ochranná bezpečnostní zóna zahrnuje prostory sloužící k uchovávání citlivých osobních údajů a důvěrných osobních údajů a informací a dokumentů, jejichž neoprávněné zveřejnění by mohlo společnosti nebo jiným osobám způsobit závažnou újmu. Do ochranné bezpečnostní zóny je povolen vstup pouze zaměstnancům, jejichž náplň práce souvisí s dokumenty a informacemi zde uchovávanými.
15.5 Vstup do ochranné bezpečnostní zóny je vždy opatřen mechanickým nebo elektronickým zámkem. Zaměstnanci jsou povinni tento vstup uzamykat.
15.6 Serverovna a další prostory, ve kterých se nacházejí úložiště velkého množství osobních údajů v elektronické podobě, vždy spadají do ochranné bezpečnostní zóny.
15.7 Rozsah a rozložení jednotlivých zón a podrobná pravidla pro přístup do nich stanoví koordinátor GDPR ve spolupráci s vedoucími pracovníky a po konzultaci se správcem budovy.
15.8 Koordinátor GDPR zajistí distribuci informací o rozložení zón a pravidlech přístupu do nich mezi zaměstnanci.
15.9 Neoprávněné šíření informací podle tohoto článku představuje bezpečnostní riziko pro společnost a může být posouzeno jako porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci ve smyslu zákona č. 262/2006 Sb., zákoník práce.

Článek XVI.
Fyzická bezpečnost osobních údajů

16.1 Prostory, ve kterých dochází ke zpracování osobních údajů, se až na výjimky stanovené touto Směrnicí nalézají vždy ve vnitřní zóně nebo v ochranné bezpečnostní zóně.
16.2 Zaměstnanci dbají na základní pravidla bezpečnosti, zejména při odchodu z prostor pečlivě zamykají dveře a kontrolují zavření oken.
16.3 Externí osoby nesmějí být ponechány v prostorách podle bodu 16.1 bez dozoru zaměstnance.
16.4 Při odchodu z prostor podle bodu 16.1 je zaměstnanec povinen zajistit, aby k jeho uživatelskému účtu nemohla přistoupit třetí osoba, například spuštěním spořiče obrazovky, který pro obnovení vyžaduje zadání uživatelského hesla.
16.5 Na všech počítačích, noteboocích a tabletech je nastaveno automatické uzamykání obrazovky s nutností opětovného zadání uživatelského hesla při nečinnosti delší než 10 minut.
16.6 V okamžiku skončení pracovní doby je zaměstnanec povinen odhlásit se ze všech informačních systémů společnosti, které využívá, a odhlásit uživatelský účet na pracovním počítači.

Článek XVII.
Uchovávání fyzických dokumentů obsahujících osobní údaje

17.1 Fyzické dokumenty obsahující osobní údaje jsou uchovávány v kancelářích, které jsou využívány zaměstnanci provádějícími danou činnost zpracování, nebo v jiných k tomu určených prostorách.
17.2 Veškeré fyzické dokumenty obsahující osobní údaje jsou v době, kdy nejsou přímo využívány, uloženy v uzamykatelných skříních.
17.3 Dokumenty jsou seskupovány podle činnosti zpracování, ke které slouží. Dokumenty sloužící různým činnostem zpracování se nemísí.
17.4 Složky dokumentů jsou viditelně označeny štítkem, na kterém je uveden alespoň název činnosti zpracování, odpovědný zaměstnanec, místo uložení dokumentů a další náležitosti dle spisového a skartačního řádu společnosti.
17.5 Složky dokumentů obsahují záznam o nahlížení do dokumentů, ve kterém se uvádí označení dokumentu, do kterého bylo nahlíženo, nahlížející osoba, osoba, která nahlížení umožnila, účel nahlížení a datum nahlížení.
17.6 Složky dokumentů dále obsahují seznam kopií dokumentů s datem pořízení a místem jejich uložení – tento záznam je také možné vést jako poznámku ve spisové službě pod číslem jednacím daného dokumentu.

Článek XVIII.
Bezpečnost informačních systémů a zálohování

18.1 IT pracovník vypracovává pro jednotlivé informační systémy a datová úložiště společnosti dokumentaci popisující bezpečnostní opatření zavedená pro daný systém nebo úložiště. Pokud v organizaci chybí vlastní IT pracovník nebo oddělení, požádá společnosti o externí odbornou pomoc, která však bude smluvně ošetřena alespoň co do oblasti ochrany osobních údajů. V takovém případě se všechny odvolávky na pracovníka IT nebo IT oddělení ve smlouvě vztahují na tohoto externího partnera.
18.2 Bezpečnostní opatření zahrnují mimo jiné řízení přístupu, šifrování, pseudonymizaci nebo používání antivirových programů.
18.3 Dokumentace obsahuje rovněž popis postupu obnovení dat při incidentu porušení zabezpečení spolu se lhůtami pro toto obnovení. Lhůty se stanovují podle úrovně důležitosti dat zpracovávaných v daném informačním systému nebo na daném úložišti.
18.4 IT pracovník stanoví způsob zálohování jednotlivých informačních systémů a datových úložišť a dobu uchování záloh.

18.5 Při zajišťování bezpečnosti informačních systémů a stanovování procesů a opatření vycházejí pracovníci IT z doporučení přijatých Radou pro IT České biskupské konference, zejména ze směrnice Politika, řízení a zajištění informační bezpečnosti, přiměřeně k velikosti společnosti a množství zpracovávaných údajů. Hledisko přiměřenosti se aplikuje také na další články týkající se přijatých technických opatření.

18.6 Pokud to možnosti společnosti dovolují, stanovují pracovníci IT bezpečnostní opatření v souladu s mezinárodními standardy ISO 27001, 27002 a 200001.

Článek XIX.
Používání notebooků, tabletů, chytrých telefonů a přenos osobních údajů

19.1 Jsou-li ke zpracování osobních údajů využívány notebooky, tablety nebo chytré telefony, je povinností zaměstnance opatřit tyto přístroje bezpečným heslem. Pokud zaměstnanec není schopen provést nastavení sám, obrátí se na pracovníky IT.

19.2 Vnitřní úložiště notebooků, tabletů a chytrých telefonů, které je využíváno k uchovávání osobních údajů, musí být zašifrováno.

19.3 Notebooky, tablety a chytré telefony jsou v případě, že je to vzhledem k velikosti společnosti a množství zpracovávaných dat přiměřené, vybaveny aplikací pro správu těchto zařízení, která umožňuje vyslat těmto zařízením pokyn k výmazu nebo zablokování v případě zjištění ztráty nebo odcizení zařízení.

19.4 Zaměstnanci jsou povinni předložit pracovníkům IT zařízení podle bodu 19.1 ke kontrole provedení nastavení.

19.5 Pokud zaměstnanci využívají ke zpracování osobních údajů přístroj v jejich soukromém vlastnictví, jsou povinni předložit příslušný přístroj pracovníkovi IT k provedení zašifrování a aplikaci příslušného zabezpečení odpovídajícího zařízením ve vlastnictví společnosti nebo přístroj ke zpracování osobních údajů dále nevyužívat. Zaměstnanci jsou rovněž povinni na těchto zařízeních využívat aktualizovaný antivirový program.

19.6 V případě, že jsou pro uchovávání nebo přenos osobních údajů využívány datové nosiče (cd, flash disky atd.) jsou dokumenty obsahující osobní údaje na tyto nosiče nahrávány v podobě archivu formátu .rar nebo .zip opatřeného heslem. Umožňuje-li to datový nosič, je šifrován celý datový nosič

19.7 Pokud jsou k přenosu osobních údajů využívány e-mailové zprávy, jsou dokumenty obsahující osobní údaje přenášeny ve formě archivu formátu .rar nebo .zip opatřených heslem. Heslo k příslušnému archivu je adresátovi e-mailové zprávy zasíláno prostřednictvím sms.

19.8 Ke vzdálenému přístupu k aplikacím a informačním systémům společnosti je vždy využíváno VPN spojení.

Článek XX.
Nakládání s dokumenty po skončení jejich užívání

20.1 Je-li ukončena činnost zpracování, pro kterou byly osobní údaje zpracovávány, a nejsou-li osobní údaje zpracovávány pro jiný účel ve smyslu čl. 6 odst. 4 GDPR, uchovávají se dokumenty obsahující osobní údaje po dobu trvání lhůt k archivaci stanovených Spisovým a skartačním řádem nebo příslušnými právními předpisy.

20.2 Po uplynutí lhůty k archivaci se dokumenty roztřídí na dokumenty určené k archivaci a dokumenty určené ke skartaci.

20.3 Fyzické dokumenty určené ke skartaci jsou zlikvidovány za využití skartovacího zařízení nebo odborné externí společnosti. S odbornou externí společností bude uzavřena smlouva o zpracování osobních údajů.

20.4 Dokumenty uchovávané v elektronické podobě jsou vymazávány tak, aby nemohlo možné jejich obnovení.

Práva subjektů údajů

Článek XXI.
Obecná ustanovení

21.1 V souvislosti se zpracováním osobních údajů svědčí subjektům údajů práva upravená v čl. 12 až 22 GDPR, a to:
   a) právo na informace o zpracování osobních údajů,
   b) právo na přístup k osobním údajům,
   c) právo na opravu,
   d) práva na výmaz,
   e) právo vznést námitku,
   f) právo na přenositelnost osobních údajů.

21.2 Při vyřizování žádostí subjektů údajů o uplatnění jejich práv postupují zaměstnanci vstřícně a se snahou v maximální možné míře vyhovět subjektům údajů při respektování příslušných ustanovení GDPR a zájmů společnosti, které nejsou v rozporu s GDPR.

21.3 Zaměstnanci jsou povinni postupovat při vyřizování žádostí subjektů údajů nebo jednotlivých úkonů vedoucích k vyřízení žádosti pečlivě a bez zbytečných průtahů.

Článek XXII.
Informační povinnost

22.1 Pokud společnost získává osobní údaje pro stanovený účel přímo od subjektu údajů, poskytne subjektu údajů informace o zpracování osobních údajů v rozsahu podle čl. 13 GDPR, a to v okamžiku získání těchto osobních údajů.

22.2 Pokud společnost získává osobní údaje z jiného zdroje než od subjektu údajů, poskytuje subjektu údajů informace o zpracování osobních údajů v rozsahu podle čl. 14 GDPR, a to při prvním kontaktu se subjektem údajů, nejpozději však do jednoho měsíce od jejich získání.

22.3 Informace o zpracování osobních údajů podle bodu 25.2 není nutné, pokud je zřejmé, že subjekt údajů už příslušné informace má.

22.4 Společnost poskytuje informace podle bodů 25.1 a 25.2 v maximálním možném rozsahu.

22.5 Informace podle bodů 25.1 a 25.2 se poskytují prokazatelnou formou, a to písemně při získání jedné kopie informace podepsané subjektem údajů, doručením informace na e-mail subjektu údajů nebo zobrazením informace jako povinného kroku v rámci webového rozhraní. Forma poskytnutí informace závisí na formě komunikace se subjektem údajů.

22.6 V rámci činnosti zpracování může být zvolen odlišný postup poskytnutí informace podle bodu 25.1 a 25.2, pokud je zajištěna doložitelnost poskytnutí informace.

Článek XXIII.
Vyřizování žádosti subjektu údajů

23.1 K přijímání žádostí subjektů údajů je příslušný koordinátor GDPR. Pokud je žádost subjektu údajů doručena jinému zaměstnanci nebo do spisovny, je povinností příslušného zaměstnance předat bez zbytečného odkladu žádost koordinátorovi GDPR.

23.2 Koordinátor GDPR vytvoří o přijaté žádosti záznam a uvědomí zodpovědného pracovníka.

23.3 Po přijetí žádosti subjektu údajů prověří koordinátor GDPR, zda je subjekt údajů bezpečně identifikovatelný. Pokud tomu tak není, vyzve subjekt údajů k prokázání identity s poučením, že při neprokázání identity nebude možné žádost vyřídit.

23.4 Předmět žádosti se posuzuje podle jejího obsahu, nikoli podle označení.

23.5 V závislosti na tom, jaké právo subjekt údajů uplatní, vyzve koordinátor GDPR odpovědné zaměstnance a pracovníky IT , aby provedli lustraci úložišť osobních údajů a sdělili mu podrobnosti o zpracování osobních údajů týkajících se žádajícího subjektu údajů. K poskytnutí těchto informací jim stanoví přiměřenou lhůtu ne delší než dva týdny.

23.6 Reakce na žádost subjektu údajů se zasílá písemně s výjimkou případů, kdy subjekt údajů požádá o jiný způsob doručení.

23.7 Datum a způsob vyřízení žádosti subjektu údajů koordinátor GDPR vyznačí do záznamu o přijetí žádosti subjektu údajů.

Incidenty porušení zabezpečení

Článek XXIV.
Hlášení porušení zabezpečení

24.1 Zjistí-li zaměstnanec porušení zabezpečení osobních údajů, informuje o tom okamžitě prokazatelným způsobem odpovědného zaměstnance, koordinátora GDPR a vedoucího pracovníka IT oddělení, pokud se porušení zabezpečení týká osobních údajů uchovávaných v elektronické podobě.

24.2 Zaměstnanec současně provede všechna opatření k zamezení pokračování porušení zabezpečení nebo jeho opakování, která mu jeho role umožňuje nebo která může fyzicky provést. O těchto opatřeních informuje osoby podle bodu 27.1.

24.3 Odpovědný zaměstnanec ve spolupráci se zaměstnancem, který porušení zabezpečení odhalil, vyplní do 24 hodin záznam o incidentu porušení zabezpečení a předá osobám podle bodu 27.1.

24.4 Koordinátor GDPR posoudí, zda je porušení zabezpečení takového charakteru, že vyžaduje hlášení Úřadu pro ochranu osobních údajů, případně subjektům údajů, jejichž osobních údajů se porušení zabezpečení týká.

24.5 Pokud je nutné provést hlášení podle bodu 27.4, provede jej koordinátor GDPR do 72 hodin od okamžiku, kdy bylo porušení zabezpečení ohlášeno, a uvede v něm všechny informace požadované podle čl. 33 GDPR.

Článek XXV.
Řešení incidentů porušení zabezpečení

25.1 Řešení incidentu porušení zabezpečení je prioritním úkolem všech zaměstnanců podílejících se na činnosti zpracování a v případě, že se týká osobních údajů zpracovávaných v elektronické podobě, také pracovníků IT oddělení.

25.2 Zaměstnanci a další osoby vyvíjejí maximální úsilí o odvrácení negativních následků porušení zabezpečení pro subjekty údajů.

25.3 Byl-li incident porušení zabezpečení ohlášen Úřadu pro ochranu osobních údajů a stanovil-li Úřad pro ochranu osobních údajů nutné kroky nebo dal-li společnosti jakákoli doporučení, jsou zaměstnanci povinni se těmito doporučeními řídit a stanovené kroky provést.

25.4 Na základě prošetření incidentu porušení zabezpečení provede odpovědný zaměstnanec opětovné posouzení vlivu činnosti na ochranu osobních údajů a stanoví opatření k zamezení opakování incidentu.

Článek XXVI.
Odpovědnost zaměstnanců

26.1 Způsobí-li zaměstnanec incident porušení zabezpečení úmyslně nebo z hrubé nedbalosti, představuje toto jednání nebo opomenutí porušení právní povinnosti vyplývající z právních předpisů vztahujících se k jím vykonávané práci zvlášť hrubým způsobem ve smyslu § 55 odst. 1 písm. b) zákona č. 262/2006 Sb., zákoník práce. Totéž platí pro případ, kdy se zaměstnanec o takové jednání nebo opomenutí pokusil, ale bez jeho přičinění k incidentu porušení zabezpečení nedošlo.

26.2 Způsobí-li zaměstnanec incident porušení zabezpečení z nedbalosti, představuje toto jednání nebo opomenutí neuspokojivý pracovní výsledek ve smyslu § 52 písm. f) zákona č. 262/2006 Sb., zákoník práce, na základě kterého bude zaměstnanec společností vyzván k jeho odstranění. Dojde-li v období 12 měsíců následujících po vyzvání společností ze strany zaměstnance k opětovnému pochybení, může být zaměstnanci dána výpověď.

26.3 Bude-li zjištěno, že zaměstnanec vystavil z nedbalosti společnost nebezpečí vzniku incidentu porušení zabezpečení, bude zaměstnanci na dobu jednoho měsíce odňato osobní hodnocení.

Kontrola ochrany osobních údajů

Článek XXVII.
Průběžná kontrola

27.1 V rámci provádění činnosti zpracování zkoumají zaměstnanci průběžně, zda zavedené procesy odpovídají GDPR, zda jsou dodržovány, zda jsou dostatečné pro ochranu osobních údajů a zda představují nejlepší dostupné řešení ochrany osobních údajů.

27.2 Koordinátor konzultuje v pravidelných intervalech vývoj rozhodovací praxe dozorového úřadu a soudů, jakož i doporučení dozorového úřadu a Evropského sboru pro ochranu osobních údajů, s odborníky na ochranu osobních údajů. Své poznatky předává odpovědným zaměstnancům a vypracovává doporučení ke zlepšení praxe ochrany osobních údajů.

27.3 Zaměstnanci IT sledují vývoj informačních technologií a informují o otázkách relevantních pro ochranu osobních údajů koordinátora GDPR. Na základě svých zjištění vypracovávají doporučení ke zlepšení praxe ochrany osobních údajů.

27.4 Odpovědní zaměstnanci předávají zaměstnancům provádějícím činnosti zpracování relevantní informace a dohlíží nad začleňováním nové praxe do činnosti zpracování.

27.5 Koordinátor GDPR je oprávněn provádět dle svého uvážení namátkové kontroly dodržování GDPR a Směrnice v rámci jakékoli činnosti zpracování.

Článek XXVIII.
Incidenční kontrola

28.1 Dojde-li k incidentu porušení zabezpečení, sestaví koordinátor GDPR ve spolupráci s odpovědným zaměstnancem zprávu shrnující příčiny a podobu incidentu. Zároveň vypracuje doporučení pro provádění ostatních činností zabezpečení pro předejití obdobnému incidentu.

28.2 Odpovědní zaměstnanci jsou povinni seznámit se se zprávou a s doporučením a podniknout příslušné kroky. Zejména zkontrolují, zda není v rámci jejich činnosti zpracování využíván tentýž proces, který zapříčinil incident porušení zabezpečení.

Článek XXIX.
Plánovaný audit

29.1 Jednou za dva roky provádí společnost komplexní audit zpracování osobních údajů. Předmětem auditu jsou zejména:
- a) kompletnost dokumentace u jednotlivých činností zpracování,
- b) dodržování GDPR a Směrnice zaměstnanci,
- c) funkčnost procesů nastavených na ochranu osobních údajů,
- d) funkčnost řízení činností zpracování.

29.2 V rámci auditu jsou vyhodnocovány zkušenosti se zpracováním osobních údajů za uplynulé dva roky.

29.3 Audit provádí koordinátor GDPR ve spolupráci nebo konzultaci s odborníkem pro ochranu osobních údajů a odpovědnými zaměstnanci. Koordinátor GDPR může provedením auditu pověřit jiného zaměstnance, který svými schopnostmi a znalostmi skýtá záruky řádného provedení auditu.

29.4 Výstupem auditu je závěrečná zpráva shrnující úroveň a problémy zpracování osobních údajů ve společnosti. Zpráva dále obsahuje doporučení pro zlepšení praxe zpracování osobních údajů a návrhy řešení zjištěných problémů.

29.5 Přílohou závěrečné zprávy je statistické shrnutí žádostí subjektů údajů o uplatnění jejich práv a jejich řešení, incidentů porušení zabezpečení a případných řízení u dozorového úřadu.

29.6 Závěrečnou zprávu předloží koordinátor GDPR statutárnímu orgánu společnosti k projednání.

Závěrečná ustanovení

Článek XXX.
Přechodná ustanovení

30.1 Statutární orgán společnosti jmenuje koordinátora GDPR do dvou týdnů ode dne účinnosti Směrnice.

30.2 Koordinátor GDPR určí odpovědné zaměstnance pro jednotlivé činnosti zpracování, které probíhají k okamžiku účinnosti Směrnice, do dvou týdnů od svého jmenování.

30.3 Odpovědní zaměstnanci vypracují záznamy o činnosti zpracování do dvou měsíců ode dne svého jmenování.

30.4 První audit ve smyslu článku 22 se uskuteční za rok od nabytí účinnosti Směrnice.

30.5 Zaměstnanci vykonávající činnost pro společnost v okamžiku účinnosti Směrnice absolvují povinné školení podle bodu 6.8 Směrnice do 6 měsíců ode dne účinnosti Směrnice. Za absolvování povinného školení se počítá také absolvování obdobného školení v období dvou měsíců před nabytím účinnosti Směrnice.

30.6 K realizaci povinností podle článků 16. a 19. bude ve lhůtě 6 měsíců od nabytí účinnosti Směrnice bude proveden úplný audit elektronických zařízení používaných v rámci činností pro společnost. Tento audit bude proveden pracovníky IT oddělení nebo externím partnerem.

Článek XXXI.

Účinnost

31.1 Směrnice nabývá účinnosti dne 25. 5. 2018.

V Kyjově dne 25. 5. 2018

Radek Šváb, ředitel, o.p.s.

_____

Jméno, funkce