SMĚRNICE Č. 1/2018 O OCHRANĚ OSOBNÍCH ÚDAJŮ

1. ÚČEL

1.1. Účelem této směrnice je stanovit základní pravidla zpracování osobních údajů ve Společnosti. Tato směrnice je jedním z organizačních opatření ochrany osobních údajů ve smyslu článku 32 GDPR.

1.2. Tato směrnice dále upravuje procesy realizace práva subjektu údajů na přístup k osobním údajům ve smyslu článku 15 GDPR a ohlašování případů porušení zabezpečení osobních údajů ve smyslu článku 33 a 34 GDPR.

2. PŮSOBNOST

2.1. Tato směrnice se vztahuje na každého Pracovníka Společnosti, když zpracovává osobní údaje nebo plní jinou činnost, která je upravena v GDPR.

2.2. Každý Pracovník, jehož se tato směrnice dotýká, bude proškolen na ochranu osobních údajů dle této směrnice a proškolení své osoby stvrdí podpisem.

3. TERMÍNY, DEFINICE A ZKRATKY

3.1. V této směrnici mají níže uvedené pojmy následující význam:

3.1.1. **DPO** – je pověřenec pro ochranu osobních údajů (Data Protection Officer) ve smyslu čl. 37 GDPR;

3.1.2. **Dozorový úřad** – Úřad pro ochranu osobních údajů;

3.1.3. **GDPR** – Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů);

3.1.4. **Osobní údaj** – jakákoliv informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;

3.1.5. **Pracovník** – je každá osoba, včetně právnických osob, která pro společnost vykonává jakoukoliv činnost, zejména zaměstnanec, externí spolupracovník, dodavatel apod.;

3.1.6. **Společnost** – je obchodní společnost STEN.cz s.r.o.;

3.1.7. **Subjekt údajů** – každá fyzická osoba, včetně osob samostatně výdělečně činných;

3.1.8. **Zpracování osobních údajů** – je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

4. ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

4.1. Statutární orgán nebo jím výslovně pověřená osoba určuje účel/y a prostředky zpracování osobních údajů pro každou evidenci ve společnosti. Tyto osoby dále určí dobu, po kterou bude každý osobní údaj zpracováván, nebo kritéria, pomocí kterých půjde tato doba určit. Osobní údaje jsou zpracovávány po dobu určenou právními předpisy nebo po dobu trvání licence ke zpracovávání osobních údajů správcem. Účel jakožto i retenční doba zpracovávání osobních údajů jsou evidovány v záznamech o činnostech zpracování vedených dle čl. 30 GDPR.

4.2. Pracovníci jsou povinni zpracovávat osobní údaje ve vztahu k subjektu údajů korektně a zákonným způsobem.

4.3. Každý pracovník smí zpracovávat osobní údaje pouze za společností určeným účelem, a to pouze společností určenými prostředky.

4.4. Pracovníci jsou oprávněni zpracovávat osobní údaje pouze v souladu s pokyny společnosti. Pracovníci smí zpracovávat pouze osobní údaje nezbytné pro plnění svých povinností vůči společnosti. Společnost za tímto účelem zřizuje pracovníkům přístup pouze k nezbytně nutným evidencím osobních údajů.

4.5. Má-li pracovník podezření, nebo dozví-li se, že jsou osobní údaje jakéhokoliv subjektu údajů nepřesné, neúplné či zastaralé, ohlásí to nadřízenému zaměstnanci společnosti nebo zaměstnanci společnosti, který s pracovníkem za společnost jedná. Není-li taková osoba, ohlásí pracovník skutečnosti.

4.6. Má-li pracovník podezření, nebo dozví-li se, že jsou osobní údaje zpracovávány déle, než je nezbytné pro účely, pro které jsou zpracovávány, ohlásí to nadřízenému zaměstnanci společnosti nebo zaměstnanci společnosti, který s pracovníkem za společnost jedná. Není-li taková osoba, ohlásí pracovník skutečnosti DPO.

5. DPO (POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ)

5.1. Společnost bude mít nepřetržitě jmenovaného DPO počínaje dnem 25. 5. 2018.

5.2. DPO je jmenován statutárním orgánem společnosti nebo pracovníkem k tomu statutárním orgánem výslovně pověřeným.

5.3. Společnost zajistí, aby DPO nedostával žádné pokyny týkající se výkonu jeho úkolů. V souvislosti s plněním svých úkolů není DPO společností propuštěn ani sankcionován. DPO je přímo podřízen statutárnímu orgánu společnosti.

5.4. V případě změny DPO pověří nový DPO vhodné pracovníky společnosti (například správce webových stránek apod.), aby dle požadavků GDPR informovali subjekty údajů, jejichž osobní údaje společnost zpracovává, o nové osobě DPO a kontaktních údajích na sebe.

5.5. DPO vykonává alespoň tyto úkoly:

5.5.1. poskytování informací a poradenství pracovníkům společnosti, kteří provádějí zpracování osobních údajů, o jejich povinnostech podle GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany osobních údajů;

5.5.2. monitorování souladu společností prováděného zpracování s GDPR, dalšími předpisy Unie nebo členských států v oblasti ochrany osobních údajů a s koncepcemi společnosti v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;

5.5.3. poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 GDPR;

5.5.4. spolupráce s dozorovým úřadem a působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování osobních údajů, včetně předchozí konzultace podle čl. 36 GDPR, a případně vedení konzultací v jakékoli jiné věci.

6. DALŠÍ POVĚŘENÉ OSOBY

6.1. Další osoby pověřené společností některými činnostmi souvisejícími se zpracováním osobních údajů, zejména prevencí incidentů, zabezpečením zpracování osobních údajů, řešením stížností a žádostí, správou systémů a dalšími činnostmi jsou uvedeny v příloze této směrnice.

6.2. Příloha č. 1 této směrnice obsahuje seznam pověřených osob s uvedením jejich rolí, aby jednotliví pracovníci vždy měli jasný přehled, na jakou osobu se obrátit v případě řešení problémů.

7. ZPRÁVA O POSOUZENÍ VLIVŮ

7.1. Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody subjektů údajů, provede společnost před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů, a to dle čl. 35 a násl. GDPR. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

7.2. Posouzení vlivu se zpracuje vždy pro:

7.2.1. 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;

7.2.2. rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10 GDPR; nebo

7.2.3. rozsáhlé systematické monitorování veřejně přístupných prostorů.

7.3. Posouzení obsahuje alespoň:

7.3.1. systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů společnosti;

7.3.2. posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;

7.3.3. posouzení rizik pro práva a svobody subjektů údajů; a

7.3.4. plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu.

7.4. Společnost si vždy vyžádá posudek DPO ke zprávě o posouzení vlivů.

7.5. Pokud ze zprávy o posouzení vlivů vyplývá, že by předmětné zpracování osobních údajů mělo za následek vysoké riziko pro práva a svobody subjektů údajů v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika, společnost konzultuje zprávu o posouzení vlivů s dozorovým úřadem. Podrobnosti určí statutární orgán společnosti.

8. KOMUNIKACE SE SUBJEKTY ÚDAJŮ

8.1. Pracovník, který obdržel v jakékoliv formě (písemně, telefonicky, osobně) jakoukoliv žádost či stížnost fyzické osoby, která se týká nebo by se mohla týkat ochrany osobních údajů, zejména žádosti ve smyslu čl. 15 - 22 GDPR, oznámí tuto skutečnost příslušné pověřené osobě.

8.2. Pokud se osobní údaje týkající se subjektu údajů získávají od subjektu údajů, poskytne pověřená osoba v okamžiku získání osobních údajů subjektu údajů informace dle čl. 13 GDPR, v případě, že osobní údaje nebyly získány od subjektu údajů, poskytne pověřená osoba tyto informace v souladu s čl. 14 odst. 3 GDPR. Povinnost poskytnout uvedené informace lze splnit odkazem na zásady ochrany osobních údajů Společnosti, které jsou dostupné na adrese www.sten.cz/internet/podminky.

8.3. Příslušná pověřená osoba vyřizuje požadavky subjektů údajů v souladu s obecnými pokyny společnosti, vždy však tak, aby žádosti subjektu údajů bylo vyhověno bez zbytečného odkladu, a aby mu byly k vyřízení jeho žádosti poskytnuty veškeré informace a v případě, že žádosti nebylo vyhověno, aby byly sděleny důvody tohoto rozhodnutí.

8.4. Neexistuje-li obecný pokyn společnosti k řešení konkrétního požadavku, vyžádá si příslušná pověřená osoba pokyn od DPO.

8.5. Ověřování identity subjektu údajů bude prováděno vždy přiměřeným způsobem, který zaručí dostatečnou identifikaci subjektu údajů s ohledem na formu podání, využitý komunikační prostředek a obsah žádosti subjektu údajů.

8.6. Všechny požadavky subjektů údajů musí být vyřízeny bez zbytečného odkladu, nikdy ne později než do 1 měsíce ode dne jejich obdržení. Pokud není možné dodržet lhůtu, příslušná pověřená osoba tuto skutečnost okamžitě oznámí nadřízenému zaměstnanci/DPO včetně uvedení důvodu, proč není možné lhůtu dodržet, a vyžádá si konzultace, jak správně postupovat dále.

8.7. V případě žádosti subjektu údajů o přístup k osobním údajům poskytne příslušná pověřená osoba subjektu údajů nejméně informaci, zda osobní údaje, které se subjektu údajů týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, poskytne mu osobní údaje subjektu údajů a informace o:

8.7.1. účelu jejich zpracování;

8.7.2. kategoriích dotčených osobních údajů;

8.7.3. příjemcích nebo kategoriích příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemcích ve třetích zemích nebo v mezinárodních organizacích;

8.7.4. plánované době, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritériích použitých ke stanovení této doby;

8.7.5. existenci práva požadovat od společnosti opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování;

8.7.6. právu podat stížnost u dozorového úřadu;

8.7.7. veškerých dostupných informacích o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;

8.7.8. skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

8.8. Informace podle tohoto článku poskytuje společnost subjektu údajů ve stejné formě, v jaké o informace subjekt údajů požádal.

8.9. V případě opakovaných žádostí subjektu údajů je subjektu údajů účtováno 50 Kč za každou opakovanou žádost.

9. OZNAMOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

9.1. Jakékoli porušení zabezpečení osobních údajů dle ustanovení čl. 4 odst. 12 GDPR společnost bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděla, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

9.2. Ohlášení dozorovému úřadu se děje prostřednictvím aplikace datové schránky.

9.3. Veškeré případy porušení zabezpečení osobních údajů společnost oznámí a konzultuje s DPO.

9.4. Ohlášení dozorovému úřadu podle tohoto článku musí přinejmenším obsahovat:

9.4.1. 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;

9.4.2. jméno a kontaktní údaje DPO nebo jiného kontaktního místa, které může poskytnout bližší informace;

9.4.3. popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

9.4.4. popis opatření, která společnost přijala nebo navrhla k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

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

9.6. Pracovníci hlásí případy porušení zabezpečení příslušným pověřeným osobám dle Přílohy č. 1 této Směrnice.

9.7. **Logování incidentů** bude na základě informací příslušných pověřených osob zpracovávat sekretariát ředitele společnosti nebo jiná pověřená osoba ve formě seznamu incidentů s popisem události.

10. VZDĚLÁVÁNÍ

10.1. Společnost zajistí pravidelná školení pracovníků dle přílohy č. 1 na zásady dodržování ochrany osobních údajů ve smyslu GDPR.

11. PROVÁDĚNÍ OZNÁMENÍ PODLE TÉTO SMĚRNICE

11.1. Ukládá-li tato směrnice povinnost osobě oznámit jakoukoliv informaci druhé osobě, provede první osoba oznámení v písemné podobě. Za tuto písemnou podobu se považuje listinný dopis nebo e-mail.

12. KONTROLA DODRŽOVÁNÍ SMĚRNICE

12.1. Dohled nad dodržováním této směrnice a závazných právních předpisů vykonává statutární orgán společnosti.

12.2. Statutární orgán společnosti slouží jako kontaktní osoba zaměstnance společnosti v otázkách bezpečnosti a ochrany osobních údajů. V případě jakýchkoli pochybností o výkladu této směrnice či rozsahu a obsahu zákonných povinností poskytuje statutární orgán závazný výklad, kterým jsou povinni se řídit.

12.3. Statutární orgán odpovídá za aktualizaci této směrnice.

13. PŘÍLOHY

13.1. Nedílnou součástí této směrnice je tato příloha: č. 1.

V Hradci Králové dne 25.05.2018

……..……..……..……..
Společnost