SMĚRNICE GŘ SPOLEČNOSTI

NÁZEV

OCHRANA OSOBNÍCH ÚDAJŮ

DATUM VYDÁNÍ	ÚČINNOST OD	POSLEDNÍ AKTUALIZACE	ČÍSLO	POČET STRAN
30. 4. 2020	1. 5. 2020		SGR/20/01	8

ZPRACOVAL

JMÉNO	FUNKCE	DATUM	PODPIS
Ing. Vladimír Mikule	TŘ	9. 4. 2020	
Ing. Nikola Gorelová	FŘ		
Ing. Kristina Schmiederová	Vedoucí HR		

SCHVÁLIL

JMÉNO	FUNKCE	DATUM	PODPIS
Ing. Milan Moravec, Ph.D.	GŘ	17. 4. 2020	

POKYNY PRO PRÁCI S DOKUMENTEM

ULOŽENÍ

Směrnice je uložena v elektronické podobě na intranetu. Podepsaný výtisk u SPJE.

SEZNÁMENÍ

Všichni zaměstnanci společnosti jsou povinni pravidelně sledovat dokumenty společnosti na intranetu a seznamovat se s novými a inovovanými dokumenty.

Se směrnicí se seznámí noví pracovníci do 1 měsíce od podpisu pracovní smlouvy a stávající zaměstnanci do 1 měsíce po datu vydání směrnice nebo její aktualizace.

OBSAH

strana

1. ÚČEL

1.1. Tato směrnice stanovuje postupy pro nakládání s osobními údaji ve společností Sweco Hydroprojekt a.s. (dále jen „**Společnost**“) s cílem zajistit ochranu osobních údajů zaměstnanců Společnosti, uchazečů o zaměstnání ve Společnosti, jejích klientů, pro které poskytuje služby, a dodavatelů, od kterých služby přijímá (dále jen „**Partner**“).

1.2. Tato směrnice nabývá účinnosti dnem uvedeného na titulní straně a vydává se na dobu neurčitou. Současně se dnem účinnosti této směrnice se ruší a nahrazuje v plném rozsahu jakékoliv předchozí verze této směrnice.

1.3. Směrnice se vztahuje na všechny zaměstnance Společnosti, jakož i členy orgánů Společnosti (dále jen „**Zaměstnanec**“). Zaměstnanci budou s touto směrnicí seznámeni způsobem ve Společnosti obvyklým.

2. SEZNAM POJMŮ A ZKRATEK

2.1. Seznam pojmů a zkratek souvisejících se zpracováním osobních údajů

Zákon	Zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů
GDPR	Nařízení č. 2016/679 Evropského parlamentu a Rady EU o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů)
Osobní údaj	Veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen **„subjekt údajů“**); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.
Subjekt údajů	Fyzická osoba, k níž se osobní údaje vztahují.
Zpracování osobních údajů	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
Evidence	Jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.
Správce	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky

	tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.
Zpracovatel	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.
Příjemce	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování.

3. ŘÍZENÍ PŘÍSTUPU VE SPOLEČNOSTI

3.1. Řízení přístupu je realizováno zejména z důvodu řízení přístupu Zaměstnanců k osobním údajům, předcházení neoprávněnému uživatelskému přístupu, modifikaci, prozrazení nebo krádeži informací a prostředků pro zpracování informací, a to na úrovni řízení fyzického i logického přístupu. Při realizaci přístupů spolupracují odpovědní Zaměstnanci zejména s IT oddělením.

3.2. Společnost zajišťuje, aby přístup k osobním údajům v informačních systémech (dále také jen „**IS**“) měli pouze Zaměstnanci, kteří dané informace potřebují pro výkon své práce – tzv. princip need-to-know (dále jen „**Oprávněný uživatel**“). Za tím účelem jsou pro každého Zaměstnance, resp. pro stejnorodou skupinu Zaměstnanců vytvořeny autorizační profily, které jsou nakonfigurovány takovým způsobem, aby byl umožněn přístup pouze k údajům a zdrojům, jež jsou potřebné k plnění povinností Zaměstnanců.

3.3. Přístupy do IS Společnost nakonfiguruje tak, aby umožňovaly přístup pouze Oprávněných Uživatelů po ověření.

3.4. Ověření se provádí na základě zadání tajného hesla a uživatelského jména, přičemž heslo je známo pouze Zaměstnanci.

3.5. Hesla nesmí být uchována v nechráněném uložišti (např. papír, běžné textové soubory). Zaměstnanec je povinen uchovat heslo v tajnosti a nikomu je nesdělovat a obecně si počínat tak, aby nemohlo dojít k vyzrazení hesla.

4. POVINNOSTI ZAMĚSTNANCŮ PŘI OCHRANĚ OSOBNÍCH ÚDAJŮ

4.1. Každý zaměstnanec Společnosti je povinen nakládat s osobními údaji zaměstnanců, uchazečů o zaměstnání, zákazníků a dodavatelů jako s důvěrnými informacemi a zachovávat o nich mlčenlivost. Zaměstnanec je povinen zachovávat mlčenlivost i po skončení pracovního poměru.

4.2. Zákaz veřejných uložišť: Osobní údaje nesmí být za žádných okolností ukládány na veřejná úložiště, ani v zašifrované formě.

4.3. Zaměstnanec není oprávněn přístupovou kartu/klíče přenechat jakékoli jiné osobě. Případnou ztrátu je povinen bez zbytečného odkladu ohlásit jako bezpečnostní incident.

4.4. Každý zaměstnanec je povinen dodržovat obecnou ***zásadu čistého stolu a prázdné obrazovky***, což znamená, že v případě nepřítomnosti Zaměstnance na pracovišti nesmí zůstat volně přístupné položené dokumenty, přenosná média a softwarově neuzamčená zařízení (počítač, tablet, mobilní telefon, …). V případě práce s osobními údaji na počítači (nebo na displeji přenosného zařízení) je Zaměstnanec povinen se ujistit, že nikdo neoprávněný nemůže tyto informace vidět.

4.5. IS a nosiče s uloženými osobními údaji musí být umístěny ve fyzicky zabezpečeném prostředí.

4.6. **Tisk a papírové dokumenty:**

4.7. Proces tisku a/nebo kopírování je fyzicky kontrolováno Zaměstnancem, který tisk/kopírování provádí, aby se zajistilo, že v tiskárnách nebo kopírovacích strojích nezůstanou žádné výtisky nebo kopie obsahující osobní údaje.

4.8. Zaměstnanec je oprávněn tisknout dokumenty obsahující osobní údaje jen v naprosto nezbytných případech pro plnění jeho pracovních povinností. Po uplynutí použitelnosti vytištěných informací je Zaměstnanec povinen provést skartaci, či jinak zabezpečit zničení výtisků.

4.9. Papírové dokumenty obsahující osobní údaje mohou být předávány pouze v uzavřené a zalepené obálce a předány nebo zaslány pouze do rukou oprávněné osoby.

4.10. Zaměstnanec je povinen ukládat všechny osobní údaje (papírová podoba nebo elektronická na přenosných médiích) do uzamykatelných skříněk nebo uzamykatelných šuplíků pracovního stolu. Klíče musí být ukládány na bezpečném místě. Dokumenty obsahující osobní údaje, které již nejsou dále potřebné, je nutné zlikvidovat bezpečným způsobem.

4.11. **Výměnná média:**

4.12. Výměnnými médii se rozumí zejména CD, DVD, BlueRay, USB flash disky, paměťové karty, diskety, externí disky, tablety, mobilní telefony. Každý zaměstnanec si je vědom toho, že s osobními údaji by měl pracovat pouze v IS, které jsou pro to určeny. Na výměnná média je Zaměstnanec oprávněn umísťovat osobní údaje jen v těch případech, kdy je to nezbytně nutné pro výkon jeho pracovní činnosti; za takto vytvořené médium je přímo odpovědný.

4.13. **Vynášení médií:**

4.14. Pokud to není nezbytně nutné z důvodu činnosti pro Společnost, nesmí osobní údaje opustit prostory Společnosti. V případě vynášení osobních údajů mimo prostory Společnosti (i v případě např. údržby) musí být média zabezpečena proti zcizení a neoprávněnému kopírování, manipulaci či přístupu k informacím na médiu umístěnými. Zejména není povoleno ponechání média v prázdném automobilu nebo na jiném místě mimo uzamčené prostory bez dozoru. Toto pravidlo platí i pro přenosné počítače.

4.15. **Odstranění důvěrných informací z médií:**

4.16. Pokud pomine důvod uložení osobních údajů na externím médiu, je Zaměstnanec odpovědný za jejich odstranění, které může mít podobu fyzického zničení nosiče nebo důsledného softwarového zničení zapsaných informací.

4.17. **Fyzická bezpečnost výměnných médií:**

4.18. Každý zaměstnanec je odpovědný za fyzickou bezpečnost výměnných a přenosných zařízení, které jsou v jeho užívání nebo mu byla předána pro plnění pracovních povinností, a za ochranu osobních údajů na nich uložených.

4.19. **Předávání osobních údajů mimo EU:**

4.20. Zaměstnanci nepředají žádné osobní údaje do zemí mimo Evropskou unii bez předchozího souhlasu smluvního oddělení nebo pověřence pro ochranu osobních údajů.

5. MINIMÁLNÍ POŽADAVKY NA PRÁCI S OSOBNÍMI ÚDAJI

5.1. Zaměstnanec je oprávněn využívat osobní údaje, se kterými bude při své práci seznámen, pouze k účelům, pro které byly poskytnuty.

5.2. Pro přenášení osobních údajů jsou voleny vždy prostředky zohledňující jejich rozsah a povahu tak, aby byla zajištěna jejich bezpečnost.

5.3. Zaměstnanci prohlédnou místnost a odstraní jakýkoli materiál obsahující osobní údaje po skončení schůzky a před opětovným použitím místnosti.

5.4. Pokud subjekt údajů uplatní vůči Společnosti práva vyplývající subjektu údajů z GDPR prostřednictvím Zaměstnance, je Zaměstnanec povinen nejpozději následující pracovní den žádost subjektu údajů předat DPO na e-mailovou adresu: SM_CZ_osobni_udaje@sweco.cz.

5.5. Zaměstnanci se zdrží komunikace o osobních údajích v rodinném kruhu (domov, rodina, příbuzní atd.) i na veřejných místech (společné místnosti a zóny na pracovišti, výtah, autobus, metro, taxi, restaurace aj.) nebo v místech, kde existuje riziko, že se osobní údaje dozví osoby, které je znát nemají

6. DPO A INCIDENTY

6.1. Společnost jmenuje pověřence pro ochranu osobních údajů (DPO), který musí být náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů. Na DPO se mohou obracet subjekty údajů ve všech záležitostech souvisejících se zpracováním jejích osobních údajů a výkonem jejích práv dle GDPR. DPO monitoruje soulad postupů ve Společnosti s GDPR a dalšími předpisy EU nebo ČR. DPO spolupracuje s dozorovým úřadem a působí jako kontaktní místo pro dozorový úřad.

6.2. **Definice incidentu:** Incidentem je každý čin nebo událost, který má za následek porušení či ohrožení ochrany osobních údajů v jakémkoli rozsahu, přičemž není rozhodující, zda incident vznikl úmyslně nebo neúmyslně, případně v důsledku porušení stanovených postupů a procedur. Incidentem jsou i objektivní okolnosti, které nastaly a zapříčinily ve svém důsledku ohrožení či narušení ochrany osobních údajů. Příkladem incidentu může být umožnění přístupu neoprávněné osoby do systémů, v nichž jsou zpracovávány osobní údaje nebo ztráta notebooku, telefonu, USB disku.

6.3. **Osoba odpovědná za hlášení incidentu:** Za hlášení je odpovědný Zaměstnanec, kterého se incident bezprostředně týká, nebo který jej zjistil jako první nebo který se o incidentu dozvěděl. V případě, že Zaměstnanec, který chce provést hlášení incidentu, prokazatelně ví, že incident již byl oznámen jiným Zaměstnancem, hlášení nepodává. V případě, že incident zjistí více osob v jednom okamžiku, hlášení podá pouze jedna osoba z nich.

6.4. Incident se hlásí DPO na e-mailovou adresu: SM_CZ_osobni_udaje@sweco.cz a zároveň na portále Sweco Service NOW. Zaměstnanec je povinen zaznamenat okolnosti incidentu.

6.5. Lhůty pro hlášení incidentů: Každý Zaměstnanec si musí být vědom skutečnosti, že vzhledem k potřebě rychlé a efektivní nápravě důsledků incidentů, jakož i vzhledem ke lhůtám stanoveným GDPR pro oznámení incidentu ze strany Společnosti Správci, dozorovému úřadu a případně subjektu údajů, je Zaměstnanec povinen incident oznámit prostřednictvím shora uvedené e-mailové adresy a portálu bez zbytečného odkladu, kdy se jej dozví, **nejpozději do 2 hodin** od tohoto zjištění.

7. ZVLÁŠTNÍ POVINNOSTI PŘI PRÁCI S VEŘEJNÝMI ZAKÁZKAMI

7.1. Zaměstnanci odpovědní za podání nabídky a realizaci veřejné zakázky jsou odpovědní i za ochranu osobních údajů při podání nabídky a realizaci veřejné zakázky.

7.2. Nabídky podané Společností za účelem získání veřejné zakázky jsou ukládány ve Společnosti pouze v elektronické podobě, v písemné podobě se nabídky nesmí ukládat ani archivovat.

7.3. Pro práci s dokumenty, kterými se prokazuje kvalifikace Společnosti, platí ustanovení této směrnice, zejména Zaměstnanci kladou důraz na omezený okruh osob, které k těmto dokumentům mají přístup. Dokumenty, kterými se prokazuje kvalifikace, se v žádném případě netisknou za jiným účelem, než je podání nabídky.

7.4. V případě, že nabídka podaná Společností, bude zadavatelem veřejné zakázky odmítnuta, zajistí Zaměstnanec odpovědný za podání nabídky v součinnosti s IT oddělením nejpozději do 5 let od odmítnutí nabídky, její likvidaci, včetně všech souvisejících dokumentů.

7.5. V případě, že nabídka podaná Společností, bude zadavatelem veřejné zakázky vyhodnocena jako nejvýhodnější a bude mezi Společností a zadavatelem veřejné zakázky uzavřena smlouva, platí pro nabídku stejné povinnosti jako při práci se smlouvami (viz následující článek).

8. ZVLÁŠTNÍ POVINNOSTI PŘI PRÁCI SE SMLOUVAMI

8.1. Zaměstnanci pracující se smlouvou uzavřenou mezi Společností a jejím partnerem jsou odpovědní za ochranu osobních údajů při uzavření a realizaci smlouvy.

8.2. Tištěná vyhotovení smluv jsou ukládány a archivovány pouze na smluvním oddělení. Ostatní Zaměstnanci jsou oprávněni pracovat s tištěným vyhotovením smlouvy či její kopií jen v nezbytně nutných případech a v nezbytně nutném rozsahu při dodržení ostatních povinností dle této směrnice.

8.3. Smlouvy jsou ukládány a archivovány elektronicky. Pro práci s elektronickou verzí smluv platí shodně ustanovení této směrnice.

8.4. Společnost zajistí, že osobní údaje obsažené v elektronicky evidovaných smlouvách (a nabídkách) budou po skončení účinnosti smlouvy a po uplynutí záruční a promlčecí doby, nestanoví-li právní předpis či příslušná smlouva delší archivační dobu, zlikvidovány. Za likvidaci elektronické verze smlouvy nese odpovědnost Zaměstnanec smluvního oddělení spolu s IT oddělením. Za likvidaci elektronické

verze nabídky (s výjimkou uzavřené smlouvy) nese odpovědnost Zaměstnanec odpovědný za podání nabídky spolu s IT oddělením.

8.5. Zaměstnanci smluvního oddělení zajistí po skončení účinnosti smlouvy a po uplynutí záruční a promlčecí doby likvidaci tištěného vyhotovení smlouvy. Totéž platí pro nabídku dle bodu 7.5. směrnice, likvidaci nabídky však zajišťují Zaměstnanci odpovědní za podání nabídky.

9. ZVLÁŠTNÍ POVINNOSTI PŘI PRÁCI S PROJEKTOVOU DOKUMENTACÍ

9.1. Zaměstnanci pracující s projektovou dokumentací jsou odpovědní za ochranu osobních údajů uvedených v projektové dokumentaci.

9.2. Zaměstnanci jsou oprávněni pracovat s tištěným vyhotovením projektové dokumentace maximálně do doby skončení výkonu autorského dozoru a jen v nezbytně nutných případech. Poté bude výtisk projektové dokumentace zlikvidován, a to zaměstnancem provádějícím autorský dozor. Projektová dokumentace je ukládána a archivována pouze elektronicky, s výjimkou uvedenou v předchozí větě.

9.3. Pro práci s elektronickou verzí projektové dokumentace shodně ustanovení této směrnice.

9.4. Elektronická verze projektové dokumentace je ukládána po dobu trvání odpovědnosti projektanta za projekt, poté Společnost zajistí její likvidaci.