PŘÍLOHA 1 - POSTUP PŘI PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ 2023

DATUM SCHVÁLENÍ: [2022-12-14]

SCHVÁLIL: PREZIDENT A GENERÁLNÍ ŘEDITEL

SPOLEČNOST SWECO AB

VLASTNÍK POLITIKY: LISA LAGERWALLOVÁ, HLAVNÍ PORADKYNĚ
AUTOR POLITIKY: BAREND VAN DEN BOS, POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ SKUPINY

Obsah

1 ÚVOD

1.1 Souvislosti a oblast působnosti

1.1.1 Všechny společnosti Skupiny Sweco při své každodenní činnosti neustále zpracovávají osobní údaje. Právní povinnosti týkající se tohoto zpracování jsou stanoveny v obecném nařízení o ochraně osobních údajů (EU) 2016/679 (dále jen "**GDPR**"), které upravuje ochranu osobních údajů. To zahrnuje pravidla týkající se opatření, která je třeba přijmout v situaci porušení ochrany osobních údajů, např. při náhodné ztrátě osobních údajů. V některých případech pravidla obsažená v nařízení GDPR vyžadují, aby společnost Sweco ohlásila porušení ochrany osobních údajů příslušnému úřadu pro ochranu osobních údajů a dotčeným osobám. Pokud je takové hlášení vyžadováno, musí být poskytnuto rychle. Vzhledem k tomu, že důsledky nedodržení GDPR by mohly být závažné, je pro společnost Sweco důležité zajistit dodržování GDPR. Společnost Sweco proto zavedla tento postup pro případ porušení zabezpečení osobních údajů (dále jen "**postup")**.

1.1.2 Účelem tohoto postupu je poskytnout návod, jak postupovat v případě porušení ochrany osobních údajů. Cílovou skupinou tohoto postupu jsou všichni zaměstnanci společnosti Sweco, včetně místních pověřenců pro ochranu osobních údajů společnosti Sweco (dále jen "**místní pověřenec pro ochranu osobních údajů")** a pověřence pro ochranu osobních údajů Skupiny Sweco (dále jen "**pověřenec pro ochranu osobních údajů Skupiny")**.

1.1.3 Tento postup je rozdělen do šesti částí. V této části je uveden krátký úvod. V oddíle 2 jsou uvedeny pokyny pro zaměstnance společnosti Sweco, jak postupovat při zjištění porušení ochrany osobních údajů. Oddíly 3 a 4 jsou určeny místním pověřencům pro ochranu osobních údajů, resp. pověřenci pro ochranu osobních údajů skupiny, a popisují, jak postupovat v případě nahlášeného porušení ochrany osobních údajů. Místní pověřenec pro ochranu osobních údajů má provést předběžné posouzení porušení ochrany údajů a poté může být povinen obrátit se na pověřence pro ochranu osobních údajů skupiny. V oddíle 5 jsou uvedeny informace, které mají být poskytnuty orgánu pro ochranu osobních údajů a jednotlivcům. Nakonec jsou v oddíle 5 popsány požadavky na dokumentaci podle GDPR v případě porušení zabezpečení údajů. Kontaktní údaje místních pověřenců pro ochranu osobních údajů a pověřence pro ochranu osobních údajů Skupiny naleznete na intranetu společnosti Sweco.

1.2 Co je únik dat?

1.2.1 GDPR definuje porušení zabezpečení osobních údajů jako "porušení zabezpečení, které vede k náhodnému nebo nezákonnému zničení, ztrátě, změně, neoprávněnému zveřejnění osobních údajů nebo přístupu k nim".

Nezáleží tedy na tom, zda k porušení ochrany osobních údajů došlo náhodou, nebo úmyslně. Dále nezáleží na tom, zda neoprávněná osoba získala přístup k osobním údajům nebo ne, protože za porušení zabezpečení údajů se považuje i náhodné zničení. Porušení ochrany osobních údajů by znamenalo například následující situace:

(i) přístup neoprávněné osoby do systému zpracovávajícího osobní údaje,
(ii) neúmyslné vymazání osobních údajů v důsledku aktualizace IT systému,
(iii) ztráta hardwaru, jako je notebook, smartphone nebo USB disk (např. zapomenutý nebo odcizený),
(iv) ztráta dešifrovacího klíče k zašifrovaným osobním údajům, která znemožňuje jejich obnovení,
(v) únik údajů od poskytovatele služeb třetí strany, pokud jsou tyto údaje zpracovávány jménem společnosti Sweco (např. poskytovatel cloudových služeb).

1.2.2 Jak je uvedeno níže, GDPR vyžaduje, aby společnost, u níž došlo k narušení bezpečnosti údajů, posoudila a případně ohlásila důsledky narušení bezpečnosti údajů. Pro dotčené osoby to může být například ztráta kontroly nad údaji, diskriminace, krádež identity, podvod, finanční ztráty, poškození pověsti a/nebo ztráta důvěrnosti. Všechny tyto okolnosti je důležité mít na paměti a posoudit, když dojde k porušení zabezpečení údajů.

2 POKYNY PRO ZAMĚSTNANCE SPOLEČNOSTI SWECO

2.1 Zaměstnanec společnosti Sweco, který zjistí porušení ochrany osobních údajů, musí toto porušení nahlásit příslušnému místnímu pověřenci pro ochranu osobních údajů do 2 hodin od zjištění porušení, a to podáním hlášení v aplikaci Service Now v části Porušení ochrany osobních údajů.

2.2 Zaměstnanec, který zjistí porušení ochrany osobních údajů, musí zdokumentovat příslušné okolnosti týkající se porušení a aktualizovat místního pověřence pro ochranu osobních údajů, jakmile se objeví nové informace, a to prostřednictvím aktualizace lístku („ticketu“) v aplikaci Service Now.

2.3 Pokud není možné poskytnout všechny požadované informace najednou, musí být dostupné informace přesto poskytnuty. Dále je nutné pokračovat ve vyšetřování porušení ochrany údajů, protože společnost Sweco bude mít pouze 72 hodin, než bude třeba informovat úřad pro ochranu údajů. Dále může být pro společnost Sweco výhodné i po uplynutí těchto 72 hodin poskytnout orgánu pro ochranu údajů další informace. Lhůty proto nesmí mít vliv na rozsah vyšetřování porušení zabezpečení údajů.

3 POKYNY PRO MÍSTNÍHO POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ

3.1 Úvod

3.1.1 Místní pověřenec pro ochranu osobních údajů je odpovědný za posouzení, zda by porušení zabezpečení údajů nahlášené zaměstnancem mělo být ohlášeno orgánu pro ochranu osobních údajů a jednotlivcům, což závisí na riziku porušení práv jednotlivců v důsledku porušení zabezpečení údajů. Místní pověřenec pro ochranu osobních údajů proto posoudí závažnost nahlášeného porušení zabezpečení údajů a klasifikuje porušení jako stupeň závažnosti 1, 2, 3 nebo 4, jak je uvedeno níže v oddíle 3.2. Při tomto posouzení musí místní inspektor ochrany osobních údajů zohlednit všechny okolnosti, např. typ porušení, povahu, citlivost a objem dotčených osobních údajů, počet dotčených fyzických osob, to, jak snadno by bylo možné fyzické osoby identifikovat, závažnost důsledků pro fyzické osoby a případné zvláštní charakteristiky fyzických osob.

3.1.2 Místní pověřenec pro ochranu osobních údajů musí vždy, bez ohledu na přidělenou úroveň závažnosti, zdokumentovat nahlášené porušení zabezpečení údajů v souladu s níže uvedeným oddílem 6.

3.2 Stupeň závažnosti 1: Žádné hlášení

3.2.1 V případě banálního porušení ochrany údajů nebo porušení, kdy nejsou dotčeny žádné osobní údaje nebo je jich dotčeno jen velmi málo, je nepravděpodobné, že by porušení ochrany údajů vedlo k ohrožení práv fyzických osob. V takovém případě není třeba porušení ohlašovat orgánu pro ochranu osobních údajů ani jednotlivcům.

3.2.2 Příklady situací, kdy lze narušení bezpečnosti údajů klasifikovat jako stupeň závažnosti 1, jsou:

(i) únik údajů, kdy jsou všechny osobní údaje již veřejně dostupné, nebo
(ii) ztráta dat, kdy jsou všechna osobní data zašifrována, dešifrovací klíč je zabezpečen a společnost Sweco je schopna použít zálohy k získání dat (upozorňujeme však, že následné zjištění, že dešifrovací klíč je kompromitován, může změnit úroveň závažnosti narušení dat).

3.2.3 Pokud místní pověřenec pro ochranu osobních údajů dojde k závěru, že porušení zabezpečení údajů je třeba klasifikovat jako porušení závažnosti 1. stupně, přijme místní pověřenec pro ochranu osobních údajů příslušná opatření a není povinen ohlásit porušení zabezpečení pověřenci pro ochranu osobních údajů Skupiny.

3.3 Stupeň závažnosti 2: nahlášení Úřadu pro ochranu osobních údajů

3.3.1 Pokud je porušení ochrany údajů závažnější a nelze dojít k závěru, že je nepravděpodobné, že by porušení ochrany údajů vedlo k ohrožení práv fyzických osob, musí být porušení ochrany údajů ohlášeno příslušnému orgánu pro ochranu osobních údajů, ledaže místní inspektor ochrany osobních údajů posoudí, že porušení ochrany údajů pravděpodobně nepovede k ohrožení dotčených fyzických osob; v takovém případě musí být toto posouzení zdokumentováno.

3.3.2 V případě, že místní inspektor ochrany osobních údajů vyhodnotí, že porušení ochrany údajů je na úrovni závažnosti 2, přijme místní inspektor ochrany osobních údajů vhodná opatření a neprodleně ohlásí porušení ochrany údajů skupinovému inspektorovi ochrany osobních údajů.

3.3.3 Pověřenec pro ochranu osobních údajů Skupiny může vydávat pokyny místnímu pověřenci pro ochranu osobních údajů. Místní pověřenec pro ochranu osobních údajů se řídí pokyny pověřence pro ochranu osobních údajů Skupiny.

3.3.4 Místní pověřenec pro ochranu osobních údajů ohlásí řešení porušení ochrany osobních údajů pověřenci pro ochranu osobních údajů Skupiny do jednoho měsíce od ohlášení orgánu pro ochranu osobních údajů.

3.4 Stupeň závažnosti 3: Hlášení orgánu pro ochranu údajů a jednotlivci

3.4.1 Pokud je pravděpodobné, že porušení ochrany údajů povede k vysokému riziku pro práva fyzických osob, musí být porušení ochrany údajů ohlášeno orgánu pro ochranu údajů a fyzickým osobám. Může se jednat o případ, kdy je zasaženo velké množství osobních údajů nebo kdy jsou zasažené údaje citlivé povahy. Příklady situací, kdy porušení zabezpečení údajů může mít 3. stupeň závažnosti (nebo 4. stupeň závažnosti), jsou následující:

(i) rozsáhlý útok ransomwaru, který znemožnil obnovení velkého množství osobních údajů,
(ii) kybernetický útok, který odhalí uživatelská jména a hesla třetím stranám, nebo
(iii) přímý marketingový e-mail týkající se určitých citlivých informací zaslaný způsobem, který umožňuje každému příjemci vidět všechny ostatní příjemce.

3.4.2 V případě, že místní inspektor ochrany osobních údajů vyhodnotí, že porušení ochrany údajů je na úrovni závažnosti 3, přijme místní inspektor ochrany

osobních údajů vhodná opatření a neprodleně ohlásí porušení ochrany údajů inspektorovi ochrany osobních údajů Skupiny.

3.4.3 Pověřenec pro ochranu osobních údajů Skupiny může vydávat pokyny místnímu pověřenci pro ochranu osobních údajů. Místní pověřenec pro ochranu osobních údajů se řídí pokyny pověřence pro ochranu osobních údajů skupiny.

3.4.4 Místní pověřenec pro ochranu osobních údajů ohlásí řešení porušení ochrany osobních údajů pověřenci pro ochranu osobních údajů Skupiny do jednoho měsíce od ohlášení orgánu pro ochranu osobních údajů a jednotlivcům.

3.5 Stupeň závažnosti 4: Nouzová situace

3.5.1 V některých velmi závažných situacích by ohlášení orgánu pro ochranu údajů a příslušným osobám nemuselo být dostačující. Pokud může porušení ochrany osobních údajů vést k velkým škodám pro jednotlivce nebo společnost Sweco, jedná se o mimořádnou událost.

3.5.2 V případě, že místní inspektor ochrany osobních údajů vyhodnotí, že porušení ochrany údajů je na úrovni závažnosti 4, přijme místní inspektor ochrany osobních údajů vhodná opatření a neprodleně ohlásí porušení ochrany údajů inspektorovi ochrany osobních údajů Skupiny. Místní pověřenec pro ochranu osobních údajů dále aktivuje krizové řízení podle příručky krizového řízení společnosti Sweco.

3.5.3 Pověřenec pro ochranu osobních údajů Skupiny vydává pokyny místnímu pověřenci pro ochranu osobních údajů. Místní pracovník pro ochranu osobních údajů se řídí pokyny pracovníka pro ochranu osobních údajů Skupiny.

3.5.4 Místní pověřenec pro ochranu osobních údajů ohlásí řešení porušení ochrany osobních údajů pověřenci pro ochranu osobních údajů Skupiny do jednoho měsíce od ohlášení orgánu pro ochranu osobních údajů a jednotlivcům.

4 POKYNY PRO POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ SKUPINY

4.1 Pověřenec pro ochranu osobních údajů Skupiny vede záznamy o hlášeních o porušení zabezpečení údajů, která obdrží od místních pověřenců pro ochranu osobních údajů.

4.2 V případech stupně závažnosti 3 může pověřenec pro ochranu osobních údajů Skupiny vydat pokyny místnímu pověřenci pro ochranu osobních údajů.

4.3 V případech stupně závažnosti 4 vydá pověřenec pro ochranu osobních údajů Skupiny pokyny místnímu pověřenci pro ochranu osobních údajů a případně aktivuje krizové řízení Skupiny podle příručky pro krizové řízení společnosti

Sweco, informuje orgán pro ochranu osobních údajů, informuje subjekty údajů a kontaktní osobu pro kybernetické pojištění.

4.4 V případech, kdy se porušení ochrany údajů stupně závažnosti 2-4 (i) týká zpracování osobních údajů prováděného společnostmi ve více než jednom členském státě EU/EHP nebo (ii) ovlivňuje nebo může významně ovlivnit fyzické osoby ve více než jednom členském státě EU/EHP, oznámí pověřenec pro ochranu osobních údajů Skupiny vedoucímu orgánu pro ochranu údajů, kterým je společnost IMY (Integritetsskyddsmyndigheten) ve Švédsku.

5 POŽADAVKY NA PODÁVÁNÍ ZPRÁV

5.1 Zprávy pro orgán pro ochranu údajů

5.1.1 Hlášení orgánu pro ochranu osobních údajů musí být podáno do 72 hodin od okamžiku, kdy bylo porušení zjištěno. Pokud však není možné nahlásit všechny informace najednou, lze je rozdělit do různých hlášení. V případě, že hlášení nelze podat do 72 hodin, musí o tom být orgán pro ochranu údajů informován a musí mu být sděleny důvody zpoždění. Doporučuje se informovat orgán pro ochranu údajů co nejdříve o tom, že všechny informace nebudou poskytnuty ve stanovené lhůtě.

5.1.2 Zpráva pro orgán pro ochranu údajů obsahuje informace o:

(i) typ narušení bezpečnosti údajů,
(ii) kategorie dotčených osob (např. zaměstnanců nebo zákazníků),
(iii) přibližný počet postižených osob,
(iv) kategorie a přibližný počet dotčených záznamů osobních údajů (např. zdravotní údaje, záznamy o vzdělání, finanční údaje),
(v) pravděpodobné důsledky narušení bezpečnosti údajů,
(vi) přijatá a/nebo navrhovaná opatření k řešení porušení zabezpečení údajů a případně ke zmírnění možných nepříznivých dopadů porušení zabezpečení údajů,
(vii) zda a jak byly tyto osoby informovány a
(viii) kontaktní údaje příslušnému pracovníkovi pro ochranu osobních údajů ve společnosti Sweco.

5.1.3 Vezměte prosím na vědomí, že orgán pro ochranu osobních údajů si může v rámci vyšetřování porušení ochrany osobních údajů vyžádat další podrobnosti.

5.2 Zprávy jednotlivcům

5.2.1 Pokud se dospěje k závěru, že je třeba zaslat jednotlivcům zprávu, informace se poskytnou bez zbytečného odkladu. Informace se poskytují jasným a

srozumitelným jazykem s cílem umožnit jednotlivcům, aby se mohli chránit. Tyto informace musí obsahovat:

(i) typ narušení bezpečnosti údajů,
(ii) možné důsledky narušení bezpečnosti údajů,
(iii) přijatá a/nebo navrhovaná opatření k řešení porušení zabezpečení údajů a případně ke zmírnění možných nepříznivých dopadů porušení zabezpečení údajů,
(iv) opatření, která by měli jednotlivci přijmout proti negativním důsledkům (např. resetování hesel), a
(v) kontaktní údaje příslušnému pracovníkovi pro ochranu osobních údajů ve společnosti Sweco.

5.2.2 Komunikace s fyzickými osobami by měla probíhat pokud možno přímo a pouze prostřednictvím zprávy týkající se porušení zabezpečení údajů. Doporučuje se nejen požádat orgán pro ochranu osobních údajů o radu ohledně toho, zda musí být fyzické osoby informovány, ale také ohledně způsobů komunikace.

5.2.3 Je třeba poznamenat, že komunikace s fyzickými osobami se nevyžaduje, pokud (i) společnost Sweco zavedla vhodná technická a organizační ochranná opatření a tato opatření byla použita na osobní údaje dotčené porušením zabezpečení osobních údajů, zejména taková, která činí osobní údaje nesrozumitelnými, (ii) společnost Sweco zajistí, že vysoké riziko pro práva fyzických osob se již pravděpodobně neprojeví, nebo (iii) kontaktování fyzických osob by vyžadovalo nepřiměřené úsilí. Ve třetím případě bude místo toho přijato veřejné sdělení nebo podobné opatření, kterým budou fyzické osoby informovány stejně účinným způsobem. Každý místní pověřenec pro ochranu osobních údajů nebo pověřenec pro ochranu osobních údajů Skupiny, který má v úmyslu uplatnit některou z těchto výjimek, by měl vždy pečlivě posoudit situaci, protože neinformování fyzických osob, když je to vyžadováno, je porušením GDPR.

5.2.4 V této souvislosti je třeba poznamenat, že orgán pro ochranu údajů může požadovat, aby společnost Sweco oznámila jednotlivcům porušení ochrany údajů, přestože se společnost Sweco rozhodla tak neučinit. Mohlo by tomu tak být buď v případě, že se orgán pro ochranu údajů na rozdíl od společnosti Sweco domnívá, že i) porušení ochrany údajů pravděpodobně povede k vysokému riziku pro práva fyzických osob, nebo ii) že se neuplatní žádná z výjimek z povinnosti informovat fyzické osoby.

6 POŽADAVKY NA DOKUMENTACI

6.1.1 Každé narušení bezpečnosti údajů musí být zdokumentováno bez ohledu na stupeň závažnosti. Dokumentace je vypracována tak, aby umožnila orgánu pro

ochranu osobních údajů dohlížet na dodržování GDPR společností Sweco, a musí obsahovat informace o každém porušení zabezpečení údajů:

(i) okolnosti narušení bezpečnosti údajů,
(ii) důsledky narušení bezpečnosti údajů,
(iii) přijatá nápravná opatření,
(iv) zda bylo porušení ohlášeno orgánu pro ochranu údajů, včetně vysvětlení, a
(v) zda byla fyzická osoba o porušení zabezpečení údajů informována, včetně vysvětlení.

6.1.2 Všechna porušení zabezpečení údajů se každoročně přezkoumávají, aby se zajistilo, že byla přijata všechna nezbytná opatření.