PŘÍLOHA 2 - POSTUP SKUPINY SWECO PRO OCHRANU SOUKROMÍ PODLE NÁVRHU DO ROKU 2023

DATUM SCHVÁLENÍ: 2022-12-14

SCHVÁLIL: PREZIDENT A GENERÁLNÍ ŘEDITEL

SWECO AB

VLASTNÍK POLICIE: Lisa Lagerwallová, hlavní poradkyně
AUTOR POLITIKY: Barend van den Bos, pověřenec pro ochranu osobních údajů skupiny

1. Úvod - účel

1.1. Společnost Sweco jako správce osobních údajů musí dodržovat zásady ochrany soukromí podle článku 25 obecného nařízení o ochraně osobních údajů (GDPR).

1.2. Účelem tohoto postupu je zvýšit povědomí o konceptu ochrany soukromí podle návrhu a poskytnout zaměstnancům společnosti Sweco návod, jak tento koncept uplatňovat v praxi. Tento postup je přílohou Zásad ochrany osobních údajů společnosti Sweco.

1.3. Tento dokument obsahuje (i) vysvětlení základních zásad ochrany soukromí podle návrhu a (ii) důležité zásady ochrany soukromí podle návrhu, které by měly být vždy dodržovány při navrhování, změně nebo pořizování systémů a procesů.

2. Zásady ochrany soukromí již od návrhu – „Privacy by Design“

2.1. Ochrana soukromí již od návrhu je proaktivní přístup k navrhování, změnám nebo pořizování systémů a procesů, který od počátku podporuje dodržování ochrany soukromí a údajů.

2.2. Při navrhování datových systémů, obchodních procesů a operací by se měl dodržovat koncept ochrany soukromí již od návrhu s tím, že ochrana údajů by měla být nedílnou součástí systému nebo procesu, aby tento systém nebo proces měl co nejmenší dopad na soukromí jednotlivců.

2.3. Výchozí nastavení by proto mělo být provedeno tak, aby bylo dodrženo maximální možné soukromí a zároveň bylo možné splnit účely zpracování osobních údajů. Zaměstnanci podílející se na navrhování systémů, procesů a operací musí brát v úvahu ochranu soukromí již v rané fázi procesu navrhování, aby bylo zajištěno, že ochrana soukromí bude do návrhu zakomponována.

2.4. Pokud je to možné, vždy používejte anonymní údaje, které nejsou podle GDPR považovány za osobní údaje. Pokud není prakticky možné použít anonymní údaje, posuďte, zda lze jména a jiné snadno identifikovatelné údaje vyměnit za pseudonymy, například ID uživatele. „Pseudonymizované“ údaje slouží ke zvýšení bezpečnosti a k tomu, aby zpracování méně zasahovalo jednotlivce.

2.5. Povinnou a včasnou součástí každého nového projektu, ať už IT/projektového nebo organizačního/provozního, by mělo být posouzení, zda a jak daný projekt ovlivní zpracování osobních údajů ve vaší organizaci. Prvním krokem je získání základních znalostí o plánovaném zpracování údajů, například jak citlivé údaje budou zpracovávány a jaké množství údajů bude zpracováváno, aby bylo možné posoudit možný dopad zpracování na jednotlivce. Na základě výsledků takového posouzení můžete přistoupit k návrhu řešení, které zohledňuje ochranu soukromí již od návrhu způsobem, který odpovídá požadavkům konkrétního projektu.

Při navrhování systémů, procesů nebo operací je třeba brát v úvahu především základní zásady ochrany údajů uvedené v GDPR.

2.6. Kromě toho by měly být zavedeny mechanismy pro naplnění práv jednotlivců podle GDPR, např. možnost (i) získat informace o zpracování, (ii) obdržet kopii registrovaných osobních údajů nebo (iii) za určitých okolností nechat údaje vymazat. Již ve fázi návrhu by měly být zváženy a zohledněny také požadavky na technická a organizační opatření, jako je šifrování a kontrola přístupu do systémů.

2.7. Závěrem lze říci, že cílem koncepce „Privacy by Design“ je, aby se integrita a ochrana dat staly přirozenou a neodmyslitelnou součástí jakéhokoli IT, obchodního nebo organizačního procesu.

Nejdůležitější zásady ochrany soukromí podle návrhu

Při pořizování nebo vývoji nových IT, obchodních nebo organizačních systémů či procesů vždy zohledněte následující důležité zásady ochrany soukromí již od návrhu. Kontrolní seznam pro jejich použití naleznete na stránce o ochraně osobních údajů skupiny Insight.

Anonymizace dat	Pokud je to možné, vždy používejte anonymní údaje (které nejsou považovány za osobní údaje). GDPR se na anonymní údaje nevztahuje. Aby byly údaje anonymní, nesmí být možné přímo ani nepřímo identifikovat žádnou fyzickou osobu za použití jakýchkoli prostředků, u nichž lze důvodně předpokládat, že by mohly být k takové identifikaci použity.
Účel zpracování, omezení účelu	Navrhněte systém nebo proces tak, aby bylo zajištěno, že zpracování údajů má vždy konkrétní, výslovný a legitimní účel, např. zabudováním funkce, která vyžaduje, aby uživatelé tento účel ověřili a/nebo popsali při registraci údajů.
Doba zpracování/uchovávání	Zajistěte, aby bylo při registraci údajů rozhodnuto o době jejich uchovávání, např. zahrnutím povinného pole pro tento účel.
Vymazání dat	Zajištění funkcí a postupů pro vymazání dat po ukončení zpracování. V některých případech může být vhodné, aby tato funkce byla výchozí automatickou funkcí, zatímco v jiných případech může mít spíše podobu automatické upomínky.
Minimalizace dat	Navrhněte systém nebo proces tak, abyste omezili zpracování osobních údajů na nezbytně nutnou míru, např. omezením volných textových polí na nezbytné minimum, navržením vstupních polí tak, aby se zabránilo registraci nadbytečných údajů.
Pseudonymizace	Zahrnout výchozí nastavení, které nahradí jména ID uživatele a jinak použije pseudonymizaci osobních údajů (tj. že identita osob není uživateli systému přístupná, pokud to není nezbytné).
Právo na přístup pro fyzické osoby	Zajistit funkčnost a postupy pro přístup fyzických osob k jejich vlastním údajům tím, že požádají o kopii zpracovávaných údajů a obdrží ji. Toho lze dosáhnout např. tím, že jednotlivci budou mít za tímto účelem sami přístup do systému.