

Informace pro provedení vstupní datové analýzy

Cílem vstupní analýzy dat je vytvořit základní přehled o stávajícím stavu zpracování osobních údajů na různých úrovních, v jednotlivých odděleních apod. a skládá se rámcově z následujících částí:

- popis, jaké všechny osobní údaje se shromažďují a z jakých důvodů
- klasifikace shromažďovaných dat podle různých kritérií, např. typu – osobní údaje, citlivé osobní údaje, veřejné osobní údaje
- identifikace, ke kterým osobním údajům je nezbytný souhlas subjektu, popis procesu získání, dokumentace a archivace takového souhlasu, postup jak prokázat jeho udělení
- zpracování tabulky (flowchart) klíčových datových toků zahrnujících osobní údaje mezi systémy a procesy
- identifikace datových toků, kdy dochází k předávání osobních údajů třetím osobám (u souhlasu je třeba na to pamatovat)
- lokalizace, kde jsou osobní údaje shromažďovány a ukládány

V zájmu získání validních údajů ve nanejvýš vhodné nominovat do týmu pro řešení projektu GDPR zástupce jednotlivých oddělení, tak aby se na analýze, mapování procesů i následném hledání a implementaci řešení podíleli přímo insideři, jinak významně roste riziko neúplných či nesprávných zjištění.

A. Účel shromažďování údajů

Posouzení důvodů a účelu sběru a zpracování osobních údajů. Je třeba zvážit všechny oblasti podnikání (jednotlivá oddělení) a identifikovat oblasti a důvody jejich shromažďování a rozsah získávaných a zpracovávaných dat. Příkladný výčet možných účelů:

1. Administrace zaměstnanců
2. Administrace klientů a obchodních partnerů (zákazníci, dodavatelé, externí spolupracovníci, studenti apod.)

3. Nabízení zboží a služeb
4. Plnění zákonných povinností (daně a účetnictví, pracovní právo)
5. Monitoring – dochází k používání technologií, které sledují údaje, jako jsou: záznamy průmyslových kamer, IP adresy, cookies, fingerprint, aplikace apod.
6. Direct marketing aktivity pro vlastní potřebu nebo třetí osoby, vytváření marketingových listů apod.
7. Evidence požadavků, stížností apod.
8. Profilování nebo hodnocení (pro sebe nebo třetí osoby) na základě osobních údajů

Již v této fázi je dobré položit si otázku, zda shromažďované údaje jsou opravdu potřeba, případně zda jsou potřeba ve stávajícím rozsahu. Cílem je obecně snížit množství shromažďovaných údajů.

B. Čí data se zpracovávají?

Pro jednotlivé výše vymezené účely je třeba hodnotit, čí data jsou zpracovávána, s přihlédnutím ke specifikům různých kategorií. Je tedy vhodné vytvořit si kategorizaci osob. Typické kategorie mohou být:

1. Zaměstnanci (potenciální, stávající, bývalí)
2. Klienti (potenciální, stávající, bývalí)
3. Obchodní partneři a dodavatelé (potenciální, stávající, bývalí)
4. Stěžovatelé a dopisovatelé
5. Děti (a jejich zákonní zástupci)
6. Jiné ...

C. Jaká data se zpracovávají?

Pro jednotlivé výše vymezené účely je třeba hodnotit, jaká data jsou zpracovávána o jednotlivých subjektech, opět je vhodné kategorizovat. Typické kategorie dat mohou být:

1. Osobní údaje (jméno, adresa, e-mail, telefon, datum narození, sexuální orientace, etnický původ atd.)
2. Finanční informace (bankovní účet, číslo kreditní karty, číslo pojištění, DIČ atd.)
3. Údaje o zdravotním stavu
4. Zvukové, obrazové a zvukově-obrazové záznamy
5. Číslo a/nebo kopie dokladů (občanský průkaz, pas, řidičský průkaz)

6. IP adresa, výrobní nebo jiná identifikační čísla el. zařízení
7. Biometrické údaje (otisky prstů, sítnice)
8. Vzdělávání a odborná příprava (CV, reference, hodnocení, pracovní povolení, absence, nemoc atd.)

Současně je třeba zkoumat, z jakých zdrojů se tyto informace získávají, což může být typicky:

1. Subjekt osobních údajů přímo
2. Třetí osoba – jakým způsobem tyto informace získáváme
3. Jiné zdroje (internet a sociální média, veřejné rejstříky apod.)

D. Právní důvod shromažďování a zpracovávání

Ve vztahu k těm jednotlivým údajům je nezbytné současně identifikovat, za jakého právního důvodu je ten který údaj zjišťován a shromažďován. Tato informace je totiž následně nezbytná pro správnou identifikaci dalšího postupu při zpracování (např. posouzení možnosti výmazu). Možné důvody jsou např.:

1. Zákonná povinnost (specifikovat nejlépe odkazem na příslušnou normu a paragraf)
2. Zákonná činnost veřejného orgánu
3. Plnění smlouvy (uzavřené se Subjektem údajů)
4. Ochrana životních zájmů Subjektů údajů
5. Oprávněné zájmy správce údajů (nutno upřesnit, o jaký zájem se jedná)
6. Souhlas (je nutné prokázat, že souhlas byl dán, a splnit omezení ohledně souhlasu)

E. Časové hledisko zpracovávání informací

Pro jednotlivé typy dat je třeba hodnotit časové konsekvence. Zpracování zahrnuje proces získání, předávání a uchovávání, a konečně vymazání údajů. Pro každý účel zpracování by mělo být definováno:

1. K jakému datu byly osobní údaje získány nebo aktualizovány (může to být i více než jednou) – tuto informaci je nutné evidovat z hlediska zahájení a běhu lhůt a dále za hlediska aktuálnosti dat.

2. Musí být stanovena doba uchovávání jednotlivých osobních údajů – ta u některých typů údajů vyplývá ze zákona (odkaz na příslušný předpis). Je nutné hodnotit, jestli je to minimální nebo maximální doba.
3. Po jakou dobu musí být zpracovatel schopen určitá data doložit třetím osobám?

F. Místo uložení a zpracování osobních údajů

S ohledem na jednotlivé účely užití je třeba nastavit, kde jsou osobní údaje uloženy (umístění může být i více), např.:

1. Fyzické záznamy (kde jsou umístěny)
2. Elektronické záznamy (kde jsou umístěny a v jakém formátu)
3. Informační systémy spravované zpracovatelem
4. Soukromá zařízení připojovaná do informačního systému zpracovatele
5. Cloudové nebo hostované služby (v jaké jurisdikci)