2.23 Informační bezpečnost a zabezpečení zpracování osobních údajů

Životní situace: Jak vyřešit požadavek na zabezpečení zpracování osobních údajů podle nové právní úpravy týkající se zpracování osobních údajů?

Popis životní situace:

Používání informačních systémů orgány veřejné moci je právně regulováno zákonem o informačních systémech veřejné správy. Jako informační systém veřejné správy se označuje informační systém, který slouží pro výkon veřejné správy. Obce v rámci tohoto zákona jsou povinny uplatňovat opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy. Obce provozují svoje informační systémy i v rámci ochrany dat v souladu s bezpečnostními principy, které jsou regulovány v zákoně o informačních systémech veřejné správy. Povinnosti vyplývající z GDPR na tyto principy navazují.

Posouzení z pohledu ochrany osobních údajů:

Povinnost zabezpečit zpracování osobních údajů je přímo stanovena v článku 32 GDPR. V praxi to znamená, že obec musí provést (s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob) vhodná technická a organizační opatření k zajištění zabezpečení odpovídající danému riziku.

Popis povinnosti zajistit zabezpečení osobních údajů:

Povinnost zajistit zabezpečení zpracování osobních údajů je přímým požadavkem vyplývajícím z článku 32 GDPR a zahrnuje povinnosti:

-
- Zajistit odpovídající technická a organizační opatření pro zabezpečení osobních údajů.
- Přihlédnout přitom ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování.
- Vyhodnotit pravděpodobnost a závažnost bezpečnostních rizik a jejich existenci zohlednit při provádění opatření.

V rámci této povinnosti se tedy projevuje jak princip proporcionality bezpečnostního řešení ve vztahu k situaci správce, tak i přístup založený na riziku, který se prolíná celým obecným nařízením.

Příklady:

- *Vstup do budovy organizace je pouze proti autentizaci pomocí vstupní identifikační karty, která je založena na zabezpečené technologii. Karty jsou současně využívány i pro dvoufaktorovou autentizaci osob pohybujících se v budově.*
- *Wifi síť, kterou obec na svých pobočkách zdarma poskytuje, je odděleným síťovým segmentem a není součástí intranetu organizace.*
- *Celé prostředí organizace je sledováno řešením SIEM zajišťujícím bezpečnostní monitoring.*
- *Personální složky jsou uloženy v kovových uzamykatelných skříních.*

Rozsah povinnosti zajistit zabezpečení údajů:

Subjekty údajů mají právo, aby bylo zpracování jejich osobních údajů bylo prováděno zabezpečenou formou. Tomu odpovídají i povinnosti správce a nutná opatření na jeho straně.

Pravidla pro naplňování povinnosti:

Bezpečnost osobních údajů má několik základních oblastí, na které by se měla každá organizace zaměřit:

- Zajištění fyzické bezpečnosti: Tato zásada mluví primárně o materiální (listinné) podobě zpracování a jejím obsahem je kontrola a zajištění bezpečnosti přístupu do prostor, kde je možné dostat se k datům, resp. k osobním údajům. Jde například o zajištění uzamykatelnosti skladovacích prostor včetně pečlivého vymezení okruhu osob, které mají k dispozici klíč, kontrolu přístupů do budovy, politiku čisté pracovní plochy a další.

- Autorizace a autentizace: Každý uživatel s přístupem k osobním údajům by měl mít přístup pouze k údajům, které nezbytně potřebuje pro výkon své agendy. Tyto přístupy a úrovně oprávnění by měly být jasně organizačně i technicky zajištěny. Mohou se prakticky promítnout například jako různé úrovně přístupových práv v aplikacích nebo adresářích, případně jako restrikce přístupů do některých částí budovy (personální archiv). Z pohledu autentizace (zajištění identifikace uživatele) je zásadní politika hesel a udržení auditní stopy o přístupu k osobním údajům.

- Ochrana proti kybernetickým incidentům a jejich detekce: V této oblasti jde převážně o ochranu pro kybernetickými hrozbami pomocí bezpečnostních nástrojů jako je například firewall, IPS, IDS nebo DLP systémy. U detekce kybernetických bezpečnostních incidentů lze pak především doporučit napojení na dohledové centrum eGovernmentu nebo na externí firmu, která bude dodatečně provádět monitoring provozních a bezpečnostních logů.

- Zavedení systému řízení informační bezpečnosti: Tato část je hlavně organizačním opatřením. Jde o vytvoření systému politik zajišťující výkon a dokumentaci agendy informační bezpečnosti v organizaci (politika hesel, politika ochrany bezpečnostního perimetru ad.)

Příklady dobré praxe při řešení modelové situace:

- ☺ *Organizace má zavedený systém řízení informační bezpečnosti včetně jeho dokumentace.*
- ☺ *Nasazení odpovídajících technických opatření kybernetické bezpečnosti.*
- ☺ *Rozdělení odpovědností za zabezpečení zpracování osobních údajů.*

Příklady špatné praxe při řešení modelové situace:

- ☹ *Informační bezpečnost není řízená a řeší se ad hoc na základě proběhlých bezpečnostních incidentů.*
- ☹ *Neexistuje dokumentace, která by zajišťovala přenositelnost informací na další pracovníky a doložitelnost bezpečnostních procesů u případné kontroly.*
- ☹ *Zaměstnanci nejsou pravidelně vzděláváni v oblasti informační bezpečnosti a ochrany osobních údajů a zvyšuje se tak riziko chyby lidského faktoru a ním spojeného porušení zabezpečení zpracování osobních údajů.*

Zdroj: Ministerstvo vnitra České republiky - https://www.mvcr.cz/gdpr/clanek/modelove-situace.aspx