Stanovení pravidel k oznamování narušení osobních údajů podle obecného nařízení k ochraně osobních údajů

Autor: Evropský výbor pro ochranu údajů – European Data Protection Board (Březen 2023)

Zdroj: Pokyny

Souhrn

Krátký souhrn celého dokumentu (Executive summary) EBPD je nezávislý evropský orgán, který přispívá k jednotnému uplatňování pravidel ochrany údajů v celé EU a podporuje spolupráci mezi orgány EU pro ochranu údajů. EBPD je zřízen GDPR a sídlí v Bruselu.

GDPR zavedlo požadavek, aby porušení ochrany osobních údajů bylo oznámeno příslušnému vnitrostátnímu dozorovému úřadu (nebo v případě přeshraničního narušení, vedoucímu orgánu) a v určitých případech oznámit narušení jednotlivcům, jejichž osobní údaje byly narušením dotčeny.

EBPD se domnívá, že oznamovací povinnost má řadu výhod. Při informování dozorového úřadu mohou správci získat radu, zda je třeba dotčené osoby informovat. Orgán dozoru může správci nařídit, aby tyto osoby o porušení informoval. Informování jednotlivců o narušení bezpečnosti umožňuje správci poskytnout informace o rizicích, která jsou výsledkem narušení, a o krocích, které tito jednotlivci mohou podniknout, aby se ochránili před jeho potenciálními důsledky. Každý plán reakce na porušení by se měl zaměřit na ochranu jednotlivců a jejich osobních údajů. Oznamování narušení by proto mělo být považováno za nástroj zvyšující dodržování předpisů ve vztahu k ochraně osobních údajů. Zároveň je třeba poznamenat, že neoznámení porušení jednotlivci nebo dozorovému úřadu může znamenat, že podle článku 83 GDPR se na správce vztahuje případná sankce.

Správcům a zpracovatelům se proto doporučuje, aby předem naplánovali a zavedli procesy, aby byli schopni odhalit a rychle zamezit narušení a posoudit riziko pro jednotlivce a poté určit, zda je nutné informovat příslušný dozorový orgán, a v případě potřeby oznámit porušení dotčeným osobám. Oznámení dozorovému orgánu by mělo být součástí tohoto plánu reakce na incident.

GDPR obsahuje ustanovení o tom, kdy a komu je třeba narušení oznámit, a také jaké informace by měly být v rámci oznámení poskytnuty. Informace požadované pro oznámení mohou být poskytovány ve fázích, ale v každém případě by správci měli jednat o jakémkoli porušení včas.

Jedním z požadavků GDPR je, že osobní údaje budou za použití vhodných technických a organizačních opatření zpracovávány způsobem, který zajistí odpovídající zabezpečení osobních údajů, včetně ochrany před neoprávněným či nezákonným zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

V souladu s tím GDPR vyžaduje, aby správci i zpracovatelé měli zavedena vhodná technická a organizační opatření k zajištění úrovně zabezpečení odpovídající riziku, které zpracovávané osobní údaje představují. Měly by zohlednit současný stav techniky, náklady na provedení a povahu, rozsah, kontext a účely zpracování, jakož i riziko různé pravděpodobnosti a závažnosti pro práva a svobody fyzických osob. GDPR také vyžaduje, aby byla zavedena veškerá vhodná technologická ochrana a organizační opatření, aby bylo možné okamžitě zjistit, zda došlo k narušení, což pak určuje, zda je splněna oznamovací povinnost.

V důsledku toho je klíčovým prvkem jakékoli politiky zabezpečení dat schopnost tam, kde je to možné, zabránit narušení a tam, kde k němu přesto dojde, na něj včas reagovat.

Z hlediska definic: Co se rozumí „zničením“ osobních údajů, by mělo být zcela jasné: zde údaje již neexistují nebo již neexistují ve formě, která je pro správce k užitku. „Poškození“ by také mělo být poměrně jasné: zde byly osobní údaje změněny, poškozeny nebo již nejsou úplné. Pokud jde o „ztrátu“ osobních údajů, mělo by to být vykládáno tak, že údaje mohou stále existovat, ale správce nad nimi ztratil kontrolu nebo přístup, nebo je již nemá v držení. Konečně neoprávněné nebo nezákonné zpracování může zahrnovat zpřístupnění osobních údajů příjemcům (nebo přístup k nim), kteří nejsou oprávněni údaje přijímat (nebo k nim mít přístup), nebo jakoukoli jinou formu zpracování, která porušuje GDPR.

Porušení lze kategorizovat podle následujících tří zásad informační bezpečnosti:

- **Porušení důvěrnosti –** pokud dojde k neoprávněnému nebo náhodnému prozrazení nebo přístupu na osobní údaje.
- **Narušení integrity –** pokud dojde k neoprávněné nebo náhodné změně osobních údajů.
- **Narušení dostupnosti –** pokud dojde k náhodné nebo neoprávněné ztrátě přístupu 18 k, nebo zničení, osobních údajů.

Je třeba také poznamenat, že v závislosti na okolnostech se porušení může týkat důvěrnosti, integrita a dostupnost osobních údajů ve stejnou dobu, jakož i jakákoli jejich kombinace. Na porušení bude vždy brán zřetel jako porušení dostupnosti, když došlo k trvalé ztrátě nebo zničení osobních údajů. **Aktuální materiál EBPD stanoví podrobná pravidla jako návod k řešení takové nastalé situace.**