OCHRANA OSOBNÍCH ÚDAJŮ PODLE EVROPSKÉHO OBECNÉHO NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (GDPR)

LEGISLATIVA REAGUJE NA RYCHLÝ TECHNOLOGICKÝ ROZVOJ A GLOBALIZACI A NUTÍ TAK FIRMY I VEŘEJNOU SPRÁVU ZMĚNIT PŘÍSTUP V OBLASTI OCHRANY OSOBNÍCH ÚDAJŮ.

Ve vazbě na technologický rozvoj umožňující jednoduché a rychlé zpracování značného množství informací dochází v posledních letech ve většině organizací ke zvětšování rozsahu shromažďovaných a sdílených osobních dat. V Evropské unii díky fungování vnitřního trhu značně roste jak objem přeshraničních toků osobních údajů, tak i výměna osobních údajů mezi veřejnými a soukromými aktéry, a to včetně fyzických osob, sdružení a podniků. V souvislosti s tím stoupají nároky na zajištění náležité ochrany zpracovávaných osobních údajů všemi zainteresovanými stranami.

[NAŘÍZENÍ GDPR]

Ve světle těchto trendů přijal Evropský parlament a Rada EU **Obecné nařízení o ochraně osobních údajů** č. 2016/679, dále jen „Nařízení" nebo i „GDPR", které začne být ve všech členských zemích účinné **od 25. května 2018**. Forma nařízení byla zvolena se záměrem sjednotit právní prostředí pro ochranu osobních údajů, kde dosud platilo 28 různých právních úprav (v ČR zákon č. 101/2000 Sb.). Cílem Nařízení je především posílení práv osob na lepší kontrolu jejich osobních údajů a zohlednění technologického vývoje při ochraně zpracovávaných dat. Přestože GDPR přináší náročnější pravidla pro správce a zpracovatele osobních údajů, stále se snaží zachovat rovnováhu mezi jejich legitimními zájmy a právem osob na ochranu soukromí.

Platí, že Nařízení považuje za zpracování osobních údajů tyto činnosti:
shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo **pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření** nebo **jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení**, tedy prakticky jakékoliv uložení, zpracování nebo přenos osobních údajů.

ZÁKLADNÍ POŽADAVKY

Základní požadavky GDPR na správce a zpracovatele osobních údajů jsou následující:

- **zavedení technických a organizačních opatření na ochranu osobních údajů (včetně hodnocení účinnosti, revizí a aktualizací)**
- **schopnost doložit soulad s Nařízením**
- **vedení záznamů o zpracování osobních údajů**
- **povinnost hlásit případy porušení zabezpečení osobních údajů dozorovému úřadu (a případně i subjektům údajů)**
- **provádění posouzení vlivu zpracování na ochranu osobních údajů (ve specifických případech)**
- **případné předběžné konzultace specifických zpracování s dozorovým úřadem**
- **jmenování pověřence pro ochranu osobních údajů (povinné pro veřejnou správu nebo při rozsáhlém zpracování osobních údajů)**

PŘI NEDODRŽOVÁNÍ NEBO PORUŠOVÁNÍ POŽADAVKŮ GDPR JSOU STANOVENY VÝRAZNÉ SPRÁVNÍ POKUTY, A TO AŽ **540 MILIONŮ KORUN** NEBO AŽ **4 PROCENTA Z ROČNÍHO GLOBÁLNÍHO OBRATU** ORGANIZACE (UPLATNÍ SE VYŠŠÍ ČÁSTKA).

[PŘÍPRAVA]

Organizace by tedy měly minimálně provést revizi:

- NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI UVNITŘ ORGANIZACE
- SOUHLASŮ, SMLUV, SMĚRNIC A INTERNÍCH DOKUMENTŮ
- NASTAVENÍ ORGANIZAČNÍCH A TECHNICKÝCH OPATŘENÍ A PROCESŮ PRO JEJICH HODNOCENÍ

[POMOC SE SPLNĚNÍM POŽADAVKŮ GDPR]

Pro zajištění souladu s Nařízením je společnost ICZ připravena pomoci:

Analýza

V rámci této skupiny služeb ICZ nabízí provedení analýzy zpracování osobních údajů ve firemních ICT systémech, tzn. identifikování, kde se údaje nachází, za jakým účelem je organizace zpracovává a zda jsou procesy zpracování v souladu s Nařízením. Dále je možné vypracování přehledové analýzy rizik mj. za účelem identifikace rizika pro práva a svobody subjektu údajů, analýzu zabezpečení informačních systémů, ve kterých jsou osobní údaje zpracovávány, a případně, podle výsledků předchozích analýz, i posouzení dopadů zpracování.

Školení

ICZ může také připravit školení, v jehož rámci se klíčoví vedoucí zaměstnanci seznámí se změnami, které GDPR přináší, což jim pomůže identifikovat případné oblasti, kam Nařízení zasáhne a podle toho reagovat na zvýšené nároky na zdroje. Další typ školení se zaměřuje přímo na zaměstnance pracující s osobními údaji, kde jim v návaznosti na interní předpisy poskytne informace o pravidlech a postupech zpracování osobních údajů a o klíčových zásadách bezpečnosti.

Příprava politik a navazujících předpisů

Pro snadnou implementaci opatření a pro pozdější prokázání shody s Nařízením ICZ vypracuje potřebné předpisy, jako jsou politiky zpracování osobních údajů (včetně např. i specifikace opatření pro žádosti, získávání a ukládání souhlasu) nebo vhodné politiky pro řízení incidentů a zotavení se z nich. Součástí služby mohou být také konzultace při implementaci požadavků politik.
V rámci této služby ICZ nabízí na základě zjištěného aktuálního stavu bezpečnostních opatření, požadavků GDPR a výsledků analýzy rizik revizi stávajících, resp. návrh nových bezpečnostních opatření. Při návrhu bude vycházet ze stávajícího stavu a bude maximálně využívat již existující opatření. Zaměří se zvláště na využití prvků zabezpečení osobních údajů zmíněných v Nařízení, jako je např. šifrování, anonymizace a pseudonymizace údajů.

Implementace bezpečnostních opatření

V této oblasti ICZ poskytuje jak služby vlastní implementace opatření (organizačních nebo technických), tak i konzultační služby v rámci implementace opatření tradičními dodavateli zákazníka. Jednotlivá opatření mohou nabývat různých forem dle možností a požadavků zákazníka – od čistě organizační formy přes formu open source nástroje až po komerční enterprise řešení. Zde je ICZ připravena v maximální míře zohlednit možnosti a potřeby zákazníka a nabídnout odpovídající formu opatření. ICZ také provádí formou interního auditu pravidelné přezkoumávání účinnosti opatření.

OBCHODNÍ KONTAKT

ICZ a.s. Na hřebenech II 1718/10
140 00 Praha 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: marketing@i.cz