AEC

SLUŽBY INFORMAČNÍ BEZPEČNOSTI

General Data Protection Regulation

Počínaje 25. květnem 2018 začne v celé Evropské unii platit Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, takzvané GDPR. Jedná se o přelomový právní akt, který sjednocuje ochranu osobních údajů v celé EU a dopadá na všechny subjekty, které osobní údaje zpracovávají.

Tato nová evropská norma vyžaduje velmi komplexní přístup k celé problematice ochrany informací, přestože je zaměřena pouze na osobní údaje. V rámci automatizovaného zpracování osobních údajů vznikají nové povinnosti vedoucí k větší transparentnosti, ale především bezpečnosti.

Toho lze docílit přijetím odpovídajících konkrétních opatření nejen v oblasti bezpečnosti IT, ale také bezpečnosti fyzické, administrativní, organizační a procesní. Je nezbytné všechny tyto oblasti komplexně propojit tak, aby celá ochrana osobních údajů fungovala jako jednolitý systém.

Nelze zajistit dostatečnou ochranu osobních údajů bez toho, aby existovala návaznost mezi řídícími dokumenty, které vycházejí z definovaných procesů a postupů a nejsou podpořeny odpovídající organizační strukturou a správně aplikovanými technologiemi.

GDPR - Nové povinnosti

Stručně a zjednodušeně řečeno dochází k významnému zpřísnění regulace v oblasti zpracování osobních údajů. Nové podmínky budou v rámci organizace vyžadovat nejen úpravu stávajících procesů, které souvisejí se zpracováním, ale budou znamenat povinnou implementaci řady dalších opatření.

Posílení práv subjektů osobních údajů	Širší informační povinnost vůči subjektům i orgánům	Výrazné zvýšení sankcí za porušení	Výslovnost souhlasu pro všechna zpracování
Povinnost hlášení úniků osobních údajů (data breaches)	**Základní novinky a změny v ochraně osobních údajů plynoucích z GDPR**		Pseudonymizace a šifrování osobních údajů
Sjednocení ochrany osobních údajů v celé EU			Nová pravidla pro vztah správce a zpracovatele včetně řetězení
Analýza dopadů na soukromí – DPIA (Data Protection Impact Assessment)	Pověřenec pro ochranu osobních údajů – DPO (Data Protection Officer)	Kodexy a certifikáty	Zvýšená ochrana osobních údajů

Řešení AEC

S využitím více než pětadvacetiletých zkušeností v oblasti bezpečnosti informací a informačních technologií nabízíme široký soubor produktů a služeb, s jejichž pomocí lze naplnit hlavní část požadavků této nové evropské legislativní normy. Ne všechna opatření musíte řešit pomocí vlastních interních zdrojů. S řadou z nich vám mohou pomoci specializovaní odborníci. takový outsourcing je v řadě případů i finančně výhodnější. Náročnost GDPR vyžaduje komplexní přístup k řízení ochrany osobních údajů. AEC nabízí unikátní propojení znalostí v oblasti systematického řízení bezpečnosti informací a nasazení vhodných bezpečnostních technologií.

Analýza souladu s požadavky GDPR

Základem pro správnou implementaci požadavků GDPR je detailní porovnání aktuálního stavu ochrany osobních údajů s požadavky definovanými nařízením. Jen tak lze zajistit efektivní implementaci všech požadavků GDPR. AEC zpracuje detailní analýzu a doporučí vhodný postup a rozsah implementace.

Návrh a implementace procesů a metodik

GDPR je založeno na principech „privacy by design“ a „risk-based aproach“. To vyžaduje nejen zavedení nových bezpečnostních procesů a metodik v rámci organizace, ale často bude mít dopad např. i v rámci architektury informačních systémů a aplikací. Jedná se zejména o postupy týkající se hlášení bezpečnostních incidentů, informační povinnosti nebo práva na výmaz. AEC navrhne a zavede procesy a metodiky customizované pro prostředí dané organizace.

Zpracování řídících dokumentů

Nezbytnou součástí ochrany osobních údajů je odpovídající řídící dokumentace (politiky, směrnice atd.), kterou organizace mj. dokládá plnění požadavků GDPR. AEC zpracuje či upraví řídící dokumenty v rozsahu odpovídajícím požadavkům GDPR s ohledem na stávající interní politiky a procesy.

Implementace technických opaření

Základním požadavkem GDPR je zajištění ochrany osobních údajů, zaručení jejich důvěrnosti, dostupnosti a integrity. K tomu je nezbytné implementovat dostatečná technická opatření k jejich zabezpečení či k identifikaci porušení bezpečnosti

Aby byla organizace v souladu s GDPR, bude si muset odpovědět na řadu elementárních otázek:

- Jaká data jsou zpracovávána a kde (všude) jsou v našich systémech uložena? Dokážeme např. „zapomenout“ osobní údaje, pokud to daný subjekt bude požadovat?
- Jak jsou data spravována a jakým způsobem jsou chráněna? Jsou chráněna dostatečně?
- Jaká interní dokumentace řeší ochranu a zpracování osobních údajů a je ve shodě s požadavky GDPR?
- Jaké role se podílejí na zpracování osobních údajů a jaké jsou jejich povinnosti? Jsou tyto povinnosti dostatečné vzhledem k požadavkům GDPR?
- Jaká je úloha třetích stran při zpracování a jak je spolupráce s nimi zajištěna (smluvně)? Jsme dostatečně zajištěni v případě možných problémů?
- Jak jsou řešeny postupy při úniku osobních údajů a při následném informování subjektů údajů a regulátora?
- Je odpovídajícím způsobem zajištěno vzdělávání a školení pracovníků?

Naše služby v oblasti GDPR

- Analýza souladu s požadavky GDPR
- Konzultace, návrh a implementace souvisejících procesů/činností/postupů do struktur organizace
- Zpracování řídících dokumentů (politik, směrnic, dalších dokumentů)
- Implementace technických nástrojů SIEM, DLP, FW/ WAF/IPS, NBA, klasifikace dokumentů
- Analýza dopadů na soukromí (Data Protection Impact Assessment)
- Outsourcing role pověřence pro ochranu osobních údajů (Data Protection Officer)
- Implementace GRC pro efektivní řízení ochrany osobních údajů a souvisejících procesů

(Data Loss Prevention, Network Behavior Analysis, SandBox, kryptografické nástroje atd.). AEC navrhne a implementuje vhodná technická řešení dle individuálních potřeb organizace.

Data Protection Impact Assessment

Analýza dopadů na osobní údaje (Data Protection Impact Assessment) je jedním ze základních nástrojů jak zajistit vysokou bezpečnost osobních údajů při jakémkoliv nakládání s osobními údaji, jako například při profilování, zpracování citlivých údajů či realizaci monitoringu veřejně přístupných prostor apod. AEC posoudí povinnost dané organizace realizovat DPIA a pokud tato povinnost vznikne, navrhne vhodný způsob implementace DPIA do stávajících (např. projektových) metodik. Dále AEC zajistí i samotné zpracování konkrétní DPIA analýzy, včetně případné konzultace s Úřadem na ochranu osobních údajů.

Pověřenec na ochranu osobních údajů - DPO

Jedním z nových požadavků GDPR je pro povinné subjekty ustanovení pověřence pro ochranu osobních údajů – Data Protection Officer. Tato role vyžaduje osobu s dostatečnou praxi a zkušeností v oblasti ochrany osobních údajů a předpokládá se jejich nedostatek na trhu. Tuto roli je možné realizovat i formou outsourcingu. AEC formou služby zajistí plnění všech povinností DPO s využitím svých zkušených a ověřených konzultantů.

Implementace GRC řešení

GDPR přináší zejména pro velké organizace zpracovávající velký objem osobních údajů mnoho dílčích povinností. Řešení GRC (Governance, Risk and Compliance) mohou být v takovém případě zásadním prvkem, který umožní efektivní řízení ochrany osobních údajů a plnění požadavků GDPR, včetně monitoringu míry souladu (compliance). AEC zajistí optimální návrh a implementaci vhodného GRC řešení nejen pro potřeby GDPR. Pro tyto účely disponuje týmem zkušených konzultantů.

Governance - Risk – Compliance (GRC)

GRC řešení pomáhá realizovat procesy v oblastech řídících procesů (IT procesy, security procesy, business procesy), řízení podnikatelských rizik (ERM, rizika bezpečnosti informací, IT rizika, dodavatelská rizika) a zajištění souladu s relevantními zákony a předpisy. Cílem GRC je dosáhnout automatizovaného a efektivního sdílení informací, provádění činností a omezení nehospodárného plýtvání zdroji.

GRC nástroje si stále častěji nacházejí cestu do všech typů organizací. Důvodem jejich pořízení jsou často různé externí tlaky, jako např. potřeba splnění požadavků zákona o kybernetické bezpečnosti (181/2014 Sb. a souvisejících vyhlášek) nebo jiných regulativních požadavků. Těchto požadavků neustále přibývá, další můžeme čekat i v souvislosti s právě přicházející evropskou regulací GDPR. Nejde však jen o splnění regulativ. GRC nástroje dokáží automatizací procesů a činností ušetřit nemalou část interních nákladů.

Implementace GRC nástroje se neskládá jenom z instalace samotného nástroje. Větší důraz je třeba klást na samotnou implementaci, která se skládá:

- Definice rozsahu implementace GRC nástroje – výběr procesů pro implementaci a jejich podrobná analýza, včetně definice požadavků organizace, identifikace datových zdrojů apod.
- Výběr nejvhodnějšího nástroje, který pokryje definované potřeby organizace.
- Instalace nástroje a jeho integrace do infrastruktury IS organizace (včetně napojení na další systémy a aplikace).
- Samotná implementace stávajících nebo optimalizovaných procesů do GRC nástroje (customizace řešení).
- Následná kontinuální podpora řešení.

GRC specialisté AEC vás provedou celou implementací GRC řešení. Našim hlavním přínosem je, že nejsme „pouze“ integrátoři a implementátoři, ale současně máme rozsáhlé zkušenosti s informační a ICT bezpečností.

Proč tuto problematiku řešit?

- Zhoršující se bezpečnostní situace klade stále větší nároky na identifikaci, hodnocení a kontinuální monitoring rizik v prostředí organizace i jejího informačního systému.
- Nové regulativy, jako je např. GDPR, nutí organizace přizpůsobovat svoje informační systémy i procesy a neustále sledovat míru plnění jednotlivých zákonných požadavků (compliance).
- Veškeré interní i externí požadavky přetavené do bezpečnostních politik je třeba pravidelně přezkoumávat a sledovat úspěšnost jejich prosazování do každodenní praxe.
- Workflow klíčových operativních procesů by mělo být standardizováno a automatizováno, přičemž data těchto procesů by měla být k dispozici a metriky by měly být průběžně vyhodnocovány.

AEC a.s.
Veveří 102
616 00 Brno, Czech Republic
Phone: +420 541 235 466

AEC a.s.
European Business Center
Dukelských hrdinů 34
170 00 Praha 7, Czech Republic
Phone: +420 267 311 402
Fax: +420 266 177 155

AEC
DATA SECURITY

www.aec.cz