AEC

SLUŽBY INFORMAČNEJ BEZPEČNOSTI

# General Data Protection Regulation

Od 25. mája 2018 začne v celej Európskej únii platiť Nariadenie Európskeho parlamentu a Rady (EU) 2016/679 o ochrane fyzických osôb v súvislosti so spracovaním osobných údajov a o voľnom pohybe týchto údajov, takzvané GDPR. Ide o prelomový právny akt, ktorý zjednocuje ochranu osobných údajov v celej EÚ a dopadá na všetky subjekty, ktoré osobné údaje spracovávajú.

Táto nová európska norma vyžaduje veľmi komplexný prístup k celej problematike ochrany informácií, hoci je zameraná iba na osobné údaje. V rámci automatizovaného spracovania osobných údajov vznikajú nové povinnosti vedúce k väčšej transparentnosti, ale predovšetkým bezpečnosti.

To možno docieliť prijatím vhodných konkrétnych opatrení nielen v oblasti bezpečnosti IT, ale aj bezpečnosti fyzickej, administratívnej, organizačnej a procesnej. Je nevyhnutné všetky tieto oblasti komplexne prepojiť tak, aby celá ochrana osobných údajov fungovala ako jednoliaty systém.

Nie je možné zabezpečiť dostatočnú ochranu osobných údajov bez toho, aby existovala náväznosť medzi riadiacimi dokumentami, ktoré vychádzajú z definovaných procesov a postupov a nie sú podporené zodpovedajúcou organizačnou štruktúrou a správne aplikovanými technológiami.

### GDPR – nové povinnosti

Stručne a zjednodušene povedané dochádza k významnému sprísneniu regulácie v oblasti spracovania osobných údajov. Nové podmienky budú v rámci organizácie vyžadovať nielen úpravu existujúcich procesov, ktoré súvisia so spracovávaním, ale budú znamenať povinnú implementáciu množstva ďalších opatrení.

| | | | |
|---|---|---|---|
| Posilnenie práv subjektov osobných údajov | Väčšia informačná povinnosť voči subjektom a orgánom | Výrazne zvýšenie sankcií pri porušení nariadenia | Výslovnosť súhlasu pre všetky spracovania |
| Povinnosť hlásenia úniku osobných údajov (data breaches) | **Základné novinky a zmeny v ochrane osobných údajov vyplývajúcich z GDPR** | | Pseudonymizácia a šifrovanie osobných údajov |
| Zjednotenie ochrany osobných údajov v celej EÚ | | | Nové pravidlá pre vzťah správcu a spracovávateľa |
| Analýza dopadov na súkromie – DPIA (Data Protection Impact Assesment) | Poverenec pre ochranu osobných údajov – DPO (Data Protection Officer) | Kódexy a certifikáty | Zvýšená ochrana osobných údajov |

## Riešenie od AEC

S využitím viac ako dvadsaťpäť rokov skúseností v informačnej bezpečnosti a informačných technológiách ponúkame širokú škálu produktov a služieb, s ktorých pomocou je možné naplniť hlavnú časť požiadaviek novej európskej legislatívnej normy. Na splnenie požiadaviek európskej únie nemusíte využívať interné zdroje. Naši špecialisti Vám pomôžu s množstvom opatrení. Tento druh outsourcingu je pre Vás finančne výhodneší. Náročnosť GDPR vyžaduje komplexný prístup k riadeniu ochrany osobných údajov. AEC ponúka unikátne prepojenie znalostí v oblasti systematického riadenia bezpečnosti informácií a nasadenie vhodných bezpečnostných technológií.

### Analýza súladu s požiadavkami GDPR

Základom pre správnu implementáciu požiadaviek GDPR je detailné porovnanie aktuálneho stavu ochrany osobných údajov s požiadavkami definovanými nariadením. Iba tak je možné zabezpečiť efektívnu implementáciu všetkých požiadaviek GDPR. AEC Vám vypracuje detailnú analýzu a odporučí vhodný postup a rozsah implementácie.

### Návrh a implementácia procesov a metodík

GDPR je založené na princípoch „privacy by design“ a „risk based approach“.To vyžaduje nielen zavedenie nových bezpečnostných procesov a metodík v rámci organizácie, ale často bude mať dopad napr.na architektúru informačného systému a aplikácií. Jedná sa hlavne o postupy hlásenia bezpečnostných incidentov, informačnej povinnosti alebo práva na výmaz. AEC navrhne a zavedie procesy a metodiky upravené pre prostredie danej organizácie.

### Spracovanie riadiacich dokumentov

Nevyhnutnou súčasťou ochrany osobných údajov je zodpovedajúca riadiaca dokumentácia (politiky, smernice atď.), ktorú organizácia mimo iného dokladá k plneniu požiadaviek GDPR s ohľadom na existujúce interné politiky a procesy.

### Implementácia technických opatrení

Základnou požiadavkou GDPR je zaistenie ochrany osobných údajov, zaručenie ich dôvernosti, dostupnosti a integrity. K tomu je nevyhnutné

**Aby bola organizácia v súlade s GDPR, bude si musieť odpovedať na niekoľko otázok:**

- Aké dáta sa spracovávajú a kde (všade) sú v systémoch uložené? Dokážeme osobné údaje vymazať pokiaľ to daný subjekt požaduje?
- Ako sú dáta spracované a akým spôsobom sú chránené? Sú dostatočne chránené?
- Aká interná dokumentácia rieši ochranu a spracovanie osobných údajov a je v zhode s GDPR?
- Aké role sa podieľajú na spracovaní osobných údajov a aké sú ich povinnosti? Sú tieto povinnosti v súlade s požiadavkami GDPR?
- Aká je úloha tretích strán pri spracovaní a ako je s nimi zaistená spolupráca (zmluvne)? Sme dostatočne zabezpečený v prípade problémov?
- Ako sú riešené postupy pri úniku osobných údajov a pri následnom informovaní subjektu údajov a regulátora?
- Vzdelávanie a školenie zamestnancov je adekvátne?

## Naše služby v oblasti GDPR

- Analýza súladu s požiadavkami GDPR
- Konzultácie, návrh a implementácia súvisiacich procesov/činností/postupov do štruktúr organizácie
- Spracovanie riadiacich dokumentov (politík, smerníc a ďalších dokumentov)
- Implementácia technických nástrojov SIEM, DLP, FW/ WAF/IPS, NBA a klasifikácie dokumentov.
- Analýza dopadov na súkromie (Data Protection Impact Assesment)
- Outsourcing role poverenca pre osobných údajov (Data Protection Officer)
- Implementácia GRC pre efektívne riadenie ochrany osobných údajov a súvisiacich procesov.

implementovať dostatočné technické opatrenia k ich zabezpečeniu alebo k identifikácií porušenia bezpečnosti (Data Loss Prevention, Network Behavior Analysis, SandBox, kryptografické nástroje atď.).

### Data Protection Impact Assesment

Analýza dopadov na osobné údaje je jedným zo základných nástrojov ako zaistiť vysokú bezpečnosť osobných údajov pri akomkoľvek spracovaní osobných údajov, ako napr. profilovanie, realizácia monitoringu verejne prístupných priestorov, atď. AEC posúdi povinnosť danej organizácie realizovať DPIA a pokiaľ táto povinnosť vznikne, navrhne vhodný spôsob implementácie DPIA do existujúcich metodík. Ďalej AEC zaistí aj samotné spracovanie konkrétnej DPIA analýzy, vrátane prípadnej konzultácie s Úradom na ochranu osobných údajov.

### Poverenec na ochranou osobných údajov – DPO

Jedným z nových požiadaviek GDPR je ustanovenie poverenca pre ochranu osobných údajov – Data Protection Officer. Táto rola vyžaduje s dostatočnou praxou a skúsenosťami v oblasti osobných údajov (predpokladá sa nedostatok na trhu). Túto rolu je možné realizovať aj formou outsourcingu. AEC formou služby zaistí plnenie všetkých povinností DPO s využitím svojich skúsených konzultantov.

### Implementácia GRC riešení

GDPR prináša hlavne pre veľké organizácie spracovávanie veľkého objemu osobných údajov. Riešenie GRC (Governance, Risk and Compliance) môžu byť v takomto prípade zásadným prvkom, ktorý umožní efektívne riadenie ochrany osobných údajov a plnenie požiadaviek GDPR, vrátane monitoringu miery súladu (compliance). AEC zaistí optimálny návrh a implementáciu vhodného GRC riešenia nielen pre potreby GDPR. Pre tieto potreby disponuje tímom skúsených konzultantov.

# Governance - Risk – Compliance (GRC)

GRC riešenie pomáha realizovať procesy v oblastiach riadiacich procesov (IT procesy, security procesy, business procesy), riadenie podnikateľských rizík (ERM, riziká bezpečností informácií, IT riziká, dodávateľské riziká) a zaistenie súladu s relevantnými zákonmi a predpismi. Cieľom GRC je dosiahnuť automatizovanie a efektívne zdieľanie informácií. GRC nástroje sa stále častejšie nachádzajú cestu do všetkých typov organizácií. Dôvodom zaobstarania sú často „externé tlaky“, ako napr. splnenie požiadaviek zákona o kybernetickej bezpečnosti alebo iná regulatívna požiadavka. Týchto požiadaviek stále pribúda, ďalšie môžeme očakávať s prichádzajúcou európskou reguláciou GDPR. Nejde však len o splnenie regulácií. GRC nástroje dokážu vďaka automatizácií procesov a činností ušetriť nemalú čiastku interných nákladov. Implementácia GRC nástroja sa neskladá len zo samotnej inštalácie. Väčší dôraz je potrebné klásť na samotnú implementáciu, ktorá sa skladá:

- Definícia rozsahu implementácie GRC nástroja – výber procesov implementácie a ich podrobná analýza, vrátane definície požiadaviek organizácie, identifikácia dátových zdrojov atď.
- Výber najvhodnejšieho nástroja, ktorý pokryje definované potreby organizácie
- Inštalácia nástroja a jeho integrácia do infraštruktúry IS organizácie (vrátane napojenia na ďalšie systémy a aplikácie)
- Samotná implementácia existujúcich procesov a optimalizovaných procesov do GRC nástroja (customizácia riešenia)
- Následná kontinuálna podpora riešenia

GRC špecialisti Vás prevedú celou implementáciou GRC riešenia. Našim hlavným prínosom je, že nie sme „iba“ integrátori a implementátori, ale súčasne máme rozsiahle skúsenosti s informačnou a ICT bezpečnosťou.

## Prečo túto problematiku riešiť?

- Zhoršujúca sa bezpečnostná situácia kladie stále väčšie nároky na identifikáciu, hodnotenie a kontinuálny monitoring rizík v prostredí organizácie a ich informačného systému.
- Nové regulácie ako napr. GDPR, nútia organizácie prispôsobovať svoje informačné systémy a procesy a neustále sledovať mieru plnenia jednotlivých zákonných požiadaviek (compliance).
- Všetky interné a externé požiadavky pretavené do bezpečnostných politík je potrebné pravidelne skúmať a sledovať úspešnosť ich presadzovania v každodennej praxi.
- Workflow kľúčových operatívnych procesov by mal byť štandardizovaný a automatizovaný, pričom dáta týchto procesov by mali byť k dispozícii a metriky by mali byť priebežne vyhodnocované.

AEC s. r. o.
Prievozská 1978/6
821 09 Bratislava
tel.: +421 254 410 283

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

AEC
DATA SECURITY

**www.aec.sk**