

GDPR



GDPR

General Data Protection Regulation kybernetická bezpečnosť pre mestá a obce

Nariadenie Európskeho parlamentu a rady Európskej únie
o ochrane osobných údajov

DATALAN

INOVÁCIE PRE ŽIVOT



25. mája 2018 vstúpi do platnosti nariadenie GDPR o ochrane osobných údajov



20 miliónov Eur alebo 4% tržieb je maximálna pokuta za nedodržanie zákona



GDPR sa týka VŠETKÝCH miest a obcí a ich podriadených organizácií, ktoré sú v EU a pracujú s osobnými údajmi



GDPR - o čo ide?

Nové nariadenie o ochrane osobných údajov GDPR (General Data Protection Regulation) predstavuje novú legislatívu, ktorá výrazne zvýši ochranu osobných údajov občanov v digitálnom svete. Cieľom nariadenia GDPR je dať európskym občanom väčšiu kontrolu nad tým, čo sa s ich údajmi deje a zároveň zjednotiť existujúce zákony o ochrane osobných údajov v rámci EU. Nové nariadenie GDPR nadobudne účinnosť **25. mája 2018** a bude platné rovnako vo všetkých členských štátoch Európskej únie a bude **povinné pre všetky mestá, obce a ich podriadené organizácie, ktoré sa nachádzajú na území Európskej únie bez ohľadu na ich veľkosť či počet obyvateľov a zamestnancov.**

Prečo je to dôležité?

Nová legislatíva GDPR prinesie nové nároky na procesnú, organizačnú a informačnú bezpečnosť. V prípade nesúladu s nariadením alebo porušenia povinností pri ochrane osobných údajov hrozí vašej organizácii astronomická pokuta, v niektorých prípadoch **až do výšky 20 miliónov EUR alebo do 4 % ročného obratu.**

Samospráva bude musieť v najbližších mesiacoch prijať technické, procesné a organizačné opatrenia a nasadiť bezpečnostné riešenia na prevenciu, detekciu, riešenie a reportovanie incidentov.

Ako vám môže pomôcť DATALAN?

DATALAN disponuje tímom skúsených bezpečnostných odborníkov, ktorí sa aktuálne spolupodieľajú na príprave viacerých organizácií na nové nariadenie GDPR. V prvom kroku tím preverí stav vašej organizácie a jej pripravenosť na nariadenie GDPR z pohľadu technológií, procesov a ľudí. Následne vykoná analýzu rizík v oblasti informačných aktív, ktoré treba chrániť. V oblasti bezpečnosti zefektívime existujúce technológie a procesy. V prípade potreby navrhujeme procesné a organizačné opatrenia a bezpečnostné nástroje, ktoré pomôžu splniť nové nariadenie GDPR.

Expertíza a konzultácie v oblasti:

- ☑ Analýza nevyhnutnej ochrany dát a implementácia opatrení a nástrojov
- ☑ vypracovanie vplyvu na ochranu osobných údajov, (Data Protection Impact Assessment)
- ☑ pseudonymizácia osobných údajov
- ☑ zabezpečenie prístupov a monitoring práce s osobnými údajmi

GDPR detailne

Ktorých organizácií verejnej správy, mestských a obecných úradov sa nariadenie GDPR týka?

Mestá, obce a podriadené inštitúcie, ktoré sledujú, analyzujú alebo ukladajú osobné dáta, musia od roku 2018 splniť oveľa náročnejšie kritéria na prácu s osobnými údajmi.

Týka sa to aj vás.

Ak vo vašom mestskom či obecnom úrade:

- zamestnávate ľudí,
- evidujete údaje o zákazníkoch, bývalých zákazníkoch, projektoch
- evidujete údaje o osobách zo strany externých dodávateľov, či partnerských organizácií, nové nariadenie sa týka aj vás.

Pre samosprávu a jej podriadené organizácie, ktoré bežne evidujú osobné údaje niekoľko tisíc obyvateľov a zamestnancov, **predstavuje príprava na nové nariadenie GDPR mesiace intenzívnej práce.** Preto je veľmi dôležité začať s prípravami už teraz a vyhnúť sa tak potenciálnemu riziku vysokej pokuty.



Čo sa premení vo fungovaní mestských a obecných úradov s novým nariadením GDPR?

Aby mestá a obce mohli doložiť súlad s GDPR, mali by prijať procesné zmeny a zaviesť opatrenia, ktoré dodržiavajú zásady ochrany osobných údajov. Tieto opatrenia sa týkajú okrem iného minimalizácie spracovaných osobných údajov, ich najrýchlejšej pseudonymizácie, transparentnosti ohľadom účelu a spracovania osobných údajov a umožneniu prístupu osôb k ich údajom.

GDPR prináša významné zmeny v právnych predpisoch EÚ v oblasti ochrany osobných údajov, z ktorých mnohé budú mať značný vplyv na fungovanie miest a obcí, napríklad:

- **Oznamovacia povinnosť pri porušení ochrany osobných údajov** – únik informácií, neautorizovaný prístup k dátam sú inštitúcie povinné ohlásiť najneskôr do 72 hodín Úradu pre ochranu osobných údajov a v niektorých prípadoch aj dotknutej osobe, či subjektom
- **Právo na vymazanie** – občania EÚ majú právo na vymazanie svojich osobných údajov zo všetkých databáz a systémov úradov, ak už nie sú potrebné na účely, na ktoré boli poskytnuté.
- **Právo na prenos osobných údajov** – pri prenose a zdieľaní osobných údajov medzi viacerými úradmi musia tieto organizácie poskytnúť zabezpečený prenos osobných údajov. Právo na prenos informácií sa dotýka aj prechodu zamestnanca do inej inštitúcie.
- **Povinnosť zaviesť pseudonymizáciu a šifrovanie dát**, ktorého účelom je mať možnosť zbierať ďalšie údaje o občanovi bez toho, aby bolo nutné poznať jeho totožnosť.
- **Zabezpečiť monitorovanie ochrany osobných údajov** – stanoviť osobu (Splnomocnenec pre ochranu osobných údajov), ktorá bude kompetentná za monitorovanie ochrany údajov a bude ako kontaktná osoba pre dozorný orgán. Nezávislosť osoby musí byť garantovaná, podlieha len vedeniu organizácie

Koho v organizácii či úrade sa nové nariadenie GDPR dotkne?



PERSONÁLNE ODDELENIE

- Nové pravidlá na evidenciu a prácu s osobnými údajmi zamestnancov a externých spolupracovníkov



KONTAKTNÉ CENTRÁ MESTSKÝCH A OBCNÝCH ÚRADOV

- Nové pravidlá na evidenciu, prácu a overovanie si osobných údajov občanov



ODDELENIA MATRIKY, ODDELENIE STAVEBNÝCH KONANÍ

- Nové pravidlá na evidenciu, prácu a overovanie si osobných údajov občanov



IT ODDELENIE, BEZPEČNOSTNÝ TÍM

- Nové bezpečnostné kritériá na systémy, v ktorých sa osobné dáta ukladajú
- Zadefinovanie, zabezpečenie a monitoring prístupov k osobným dátam
- Prísnejšie zabezpečenie pred únikom osobných dát
- Zdieľanie vybraných osobných dát s externými organizáciami bude možné len v súlade s bezpečnostnými kritériami GDPR



MANAŽMENT

- Optimalizácia existujúceho alebo zavedenie nového bezpečnostného systému pre vybrané agendy miest a obcí, ktoré vyžadujú prácu s osobnými údajmi
- Zriadiť nezávislú kontrolnú funkciu DPO (DATA Protection Officer) – Splnomocnenec pre ochranu osobných údajov, ktorý bude dohliadať na správne zaobchádzanie s osobnými údajmi a hlásiť možné úniky dát alebo porušenie zákona

Čo sú to osobné údaje?

Osobné údaje sú akékoľvek dáta o osobe, na základe ktorých je možné túto osobu identifikovať. Typickým príkladom sú:

- Meno a priezvisko
- Pohlavie
- Dátum narodenia
- Okrem iného aj IP adresa a fotografický záznam

V niektorých prípadoch sa za osobné údaje považujú aj e-mailová adresa, telefónne číslo či identifikačné údaje o osobe vydané štátom.

Čo je to pseudonymizácia osobných údajov?

Jedná sa o proces skrytia identity, ktorého účelom je mať možnosť zbierať ďalšie údaje o osobe bez toho, aby bolo nutné poznať jeho totožnosť.



Ako sa dobre pripraviť na nové nariadenie GDPR?

Príprava na nariadenie GDPR zahŕňa komplexnú agendu analýz a procesov, s ktorým vám rád pomôže tím skúsených bezpečnostných odborníkov z DATALANu. Na základe analýzy rizík v oblasti informačných aktív navrhujeme procesné a organizačné opatrenia a bezpečnostné nástroje, ktoré vám pomôžu splniť požiadavky nariadenia GDPR. Keďže sa jedná o rozsiahlu agendu, je v jednotlivých fázach navrhnutý aj orientačný časový harmonogram.

1

POVEDOMIE A ZBER INFORMÁCIÍ Január – Máj 2017

Odporúčanie: Všetci pracovníci, ktorých sa príprava na nariadenie GDPR dotkne, by mali byť včas a presne informovaní o dôležitosti a dopade nariadenia GDPR na vašu organizáciu. Zabezpečená by mala byť tiež súčinnosť všetkých zainteresovaných strán.

Fáza 1 zahŕňa audit osobných údajov a odpovede (nielen) na tieto otázky:

- Na ktoré činnosti sa v mestskom/obecnom úrade používajú osobné dáta?
- Kde sa osobné údaje ukladajú?
- Ako sú zabezpečené, a ako sú zálohované?
- Kto má k nim prístup, a ako je tento prístup monitorovaný?
- Ako sú osobné dáta zdieľané v rámci úradu, s externými organizáciami a ďalšími inštitúciami?
- Kto je zodpovedný za stratu osobných dát?
- Sú súčasné IT systémy a procesy v súlade s novým nariadením GDPR?
- Je váš úrad pripravený na nové práva osôb? (právo na vymazanie, právo preniesť osobné údaje v súlade s novým nariadením GDPR?)

DATALAN ako technologický partner zabezpečí:

- inventarizáciu informačných aktív
- kategorizáciu informačných aktív vrátane identifikácie väzieb informačných aktív na nariadenie o ochrane osobných údajov a príslušnú legislatívu
- zmapovanie služieb a činností poskytovaných občanom a zamestnancom úradu (vedenie matriky, oddelenie stavebných konaní, vedenie personálnej a mzdovej agendy a pod.)
- posúdenie informačných systémov a ich používania a tiež osôb a tretích strán, ktorý majú prístup k osobným údajom spracúvaným obcou (poskytovatelia softvérov, stravných lístkov, externé audítorské spoločnosti, spoločnosť zabezpečujúca vývoz odpadu a podobne)

2

IDENTIFIKÁCIA NEZHÔD Máj – August 2017

Odporúčanie: V tejto fáze je dôležité stanoviť si oblasti, ktoré bude potrebné upraviť v súlade s novými legislatívnymi požiadavkami. V organizáciách je často potrebné upraviť procesy, spôsob spracovania citlivých osobných dát. Takisto je nevyhnutné identifikovať oblasti s vysokým rizikom a z technologického pohľadu je potrebné preveriť kompatibilitu IT systémov s novým nariadením, ako napríklad prenos či vymazanie dát ale aj pár praktických opatrení, ako napríklad skrátenie časových intervalov pri požiadavke o prístup k dátam.

DATALAN ako technologický partner zabezpečí:

- rizikovú analýzu / vyhodnotenie rizík s dopadom na činnosť organizácie
- GAP analýzu aktuálneho stavu voči požadovanému riešeniu

3

NÁVRH OPATRENÍ August – December 2017

Odporúčanie: Na základe analýzy sa vypracuje návrh opatrení z pohľadu technológií a procesov a adekvátny spôsob monitorovania prístupu a spracovania citlivých dát. Z technologického pohľadu sa jedná napríklad o posilnenie technických a bezpečnostných nástrojov, pre niektoré prípady použitie enkryptovaných technológií a podobne. Z organizačného pohľadu bude potrebné vypracovať stratégiu a praktický manuál pre rôzne situácie, ako napríklad pravidlá pre monitorovanie verejných priestorov a návštev, ale aj presný postup krokov v prípade neželaného úniku dát a podobne.

DATALAN ako technologický partner zabezpečí:

- vypracovanie bezpečnostného projektu
- zoznam technologických opatrení s navrhovanými riešeniami
- zoznam procesných opatrení s popisom jednotlivých procesov

4

IMPLEMENTÁCIA December 2017 – Marec 2018

Odporúčanie: V tejto fáze je potrebné zaviesť organizačné, procesné a technologické zmeny a nastaviť bezpečnostné opatrenia. V jednoduchosti je krása. Pokiaľ je možné niečo v systéme zjednodušiť, teraz je príležitosť tak urobiť. Takisto je dôležité zrevidovať a aktualizovať bezpečnostnú politiku a interné nariadenia.

DATALAN ako technologický partner zabezpečí:

- vykonanie zmien v existujúcich technológiách
- obstarávanie a nasadenie riešení ako napríklad:
 - o riadenie a monitorovanie aktív s osobnými údajmi
 - o archivácia záznamov
 - o pseudonymizácia a šifrovanie osobných údajov
 - o zabezpečenie dôvernosti integrity, dostupnosti a odolnosti systémov spracúvania a služieb
 - o schopnosť rýchlej obnovy dostupnosti osobných údajov v prípade incidentu
- nastavenie procesov
- školenie zamestnancov

5

KOMUNIKÁCIA A PREVÁDZKA Marec 2018 – Máj 2018

Odporúčanie: V tejto fáze je dôležité transparentne a zrozumiteľne komunikovať dôležité zmeny pre ľudí v rámci organizácie, ktorých sa nové nariadenie GDPR dotkne. Z technologického pohľadu je potrebné zabezpečiť pravidelnú aktualizáciu a testovanie opatrení.

DATALAN ako technologický partner zabezpečí:

- proces pravidelného testovania prijatých opatrení a ich pravidelná aktualizácia

DATALAN, a.s.
Galvaniho 17/A
821 04 Bratislava
Tel.: 02 502 577 77
Fax: 02 502 577 00

 www.datalan.sk/security