GDPR

General Data Protection Regulation

kybernetická bezpečnosť pre poskytovateľov zdravotnej starostlivosti

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 firiem a organizácií, ktoré pôsobia 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 spoločnosti, ktoré pôsobia na území Európskej únie bez ohľadu na ich veľkosť či počet 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 inštitúcii, nemocnici, či poisťovni **astronomická pokuta,** v niektorých prípadoch **až do výšky 20 miliónov EUR alebo do 4 % ročného obratu.**

Poskytovatelia zdravotnej starostlivosti budú 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 spoločností 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 zefektívnime existujúce technológie a procesy. V prípade potreby navrhneme 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
- ☑ analýza účelov, právneho základu a rozsahu spracúvania osobných údajov
- ☑ vypracovanie vplyvu na ochranu osobných údajov, (Data Protection Impact Assessment)
- ☑ pseudonymizácia osobných údajov
- ☑ zabezpečenie prístupov a monitoring práce s osobnými údajmi

GDPR detailne

Koho sa nariadenie GDPR týka?
Poskytovateľov zdravotnej starostlivosti, ktorí sledujú, analyzujú alebo ukladajú osobné dáta, musia od roku 2018 splniť oveľa náročnejšie kritériá na prácu s osobnými údajmi.

Týka sa to aj vás.
Ak vo vašej organizácii:
- zamestnávate ľudí,
- evidujete údaje o klientoch, pacientoch a projektoch
- evidujete údaje o osobách zo strany externých dodávateľov, či partnerských organizácií,

nové nariadenie sa týka aj vás.

Pre poskytovateľov zdravotnej starostlivosti, ktorí bežne evidujú osobné údaje niekoľko tisíc pacientov 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.

Aké zmeny vyplývajú pre poskytovateľov zdravotnej starostlivosti s novým nariadením GDPR?
Aby nemocnice, poisťovne a ďalšie inštitúcie v oblasti zdravotníctva 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, v transparentnosti ohľadom účelu a spracovania osobných údajov a umožneniu prístupu osôb k ich údajom.

GDPR prináša významné zmeny v právnych predpisov EÚ v oblasti ochrany osobných údajov, z ktorých mnohé budú mať značný vplyv na fungovanie poskytovateľov zdravotnej starostlivosti, napríklad:
- **Oznamovacia povinnosť pri porušení ochrany osobných údajov** – únik informácií, neautorizovaný prístup k dátam sú organizácie povinné ohlásiť najneskôr do 72 hodín Úradu pre ochranu osobných údajov a v niektorých prípadoch aj dotknutej osobe, či subjektom
- **Právo na vymazanie** – klienti poskytovateľov zdravotnej starostlivosti majú právo na vymazanie svojich osobných údajov, ak už nie sú potrebné na účely, na ktoré boli poskytnuté.
- **Právo na prenos osobných údajov** – pri prechode klienta k inému poskytovateľovi zdravotnej starostlivosti, či ambulantnému lekárovi musia títo poskytovatelia poskytnúť zabezpečený prenos osobných údajov k ďalšej inštitúcii. Právo na prenos informácií sa dotýka aj prechodu zamestnanca do inej organizácie.
- **Povinnosť zaviesť pseudonymizáciu a šifrovanie dát** – účelom je mať možnosť zbierať ďalšie údaje o občanovi bez toho, aby bolo nutné poznať jeho totožnosť.
- **Zabezpečiť monitorovanie ochrany osobných údajov** – stanoviť osobu, ktorá bude kompetentná za monitorovanie ochrany údajov a bude ako kontaktná osoba pre dozorný orgán. Nezávislosť osoby musí byť garantovaná, podlieha len vedeniu spoločnosti

Spracovanie osobných údajov o zdraví
Spracovanie osobných údajov o zdraví na účely vykonávania verejného zdravotného poistenia je povolené, ak je nevyhnutné na účely preventívneho alebo pracovného lekárstva, posúdenia pracovnej spôsobilosti zamestnanca, lekárskej diagnózy, poskytovania zdravotnej alebo sociálnej starostlivosti alebo liečby. Tieto údaje môže spracovať poskytovateľ zdravotnej starostlivosti, zdravotná poisťovňa, alebo odborne spôsobilá osoba vykonávajúca služby súvisiace s poskytovaním zdravotnej starostlivosti alebo dohľad nad zdravotnou starostlivosťou, ktorá je viazaná povinnosťou mlčanlivosti.

Koho v rámci poskytovateľov zdravotnej starostlivosti sa nové nariadenie GDPR dotkne?

ŠPECIALIZOVANÉ ODDELENIA
- Nové pravidlá na evidenciu a prácu s osobnými údajmi pacientov a klientov, ako aj bývalých pacientov u poskytovateľov zdravotnej starostlivosti

AMBULANCIE, EXTERNÉ PRACOVISKÁ
- Nové pravidlá na evidenciu, prácu a overovanie si osobných údajov pacientov, nových klientov, ako aj bývalých pacientov u poskytovateľov zdravotnej starostlivosti

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

MANAŽMENT
- Optimalizácia existujúceho alebo zavedenie nového bezpečnostného systému pre vybrané agendy bánk a poisťovní, 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 navrhneme 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

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 inštitúcii 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 poskytovateľov zdravotnej starostlivosti, s externými obchodnými partnermi a ďalšími inštitúciami?
- Kto je zodpovedný za stratu osobných dát?
- Sú súčasné IT systémy a procesy v súlade s novým nariadením GDPR?
- Je vaša organizácia pripravená 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

2

IDENTIFIKÁCIA NEZHÔD

Odporúčanie: V tejto fáze je dôležité stanoviť si oblasti, ktoré bude potrebné upraviť v súlade s novými legislatívnymi požiadavkami. Vo firmách je často potrebné upraviť procesy, spôsob spracovania citlivých osobných dát. Takisto je nevyhnutné identifikovať oblasti s vysokým rizikom. Z technologického pohľadu je potrebné preveriť kompatibilitu a súlad IT systémov s novým nariadením, ako napríklad prenos či vymazanie dát ale aj nahlasovanie a riešenie bezpečnostných incidentov.

DATALAN ako technologický partner zabezpečí:

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

3

NÁVRH OPATRENÍ

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 napríklad jedná 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:

- Zoznam technologických opatrení s navrhovanými riešeniami
- Zoznam procesných opatrení s popisom jednotlivých procesov

4

IMPLEMENTÁCIA

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:
  - riadenie a monitorovanie aktivít s osobnými údajmi
  - archivácia záznamov
  - pseudonymizácia a šifrovanie osobných údajov
  - zabezpečenie dôvernosti integrity, dostupnosti a odolnosti systémov spracovania a služieb
  - schopnosť rýchlej obnovy dostupnosti osobných údajov v prípade incidentu
- Nastavenie procesov
- Školenie zamestnancov

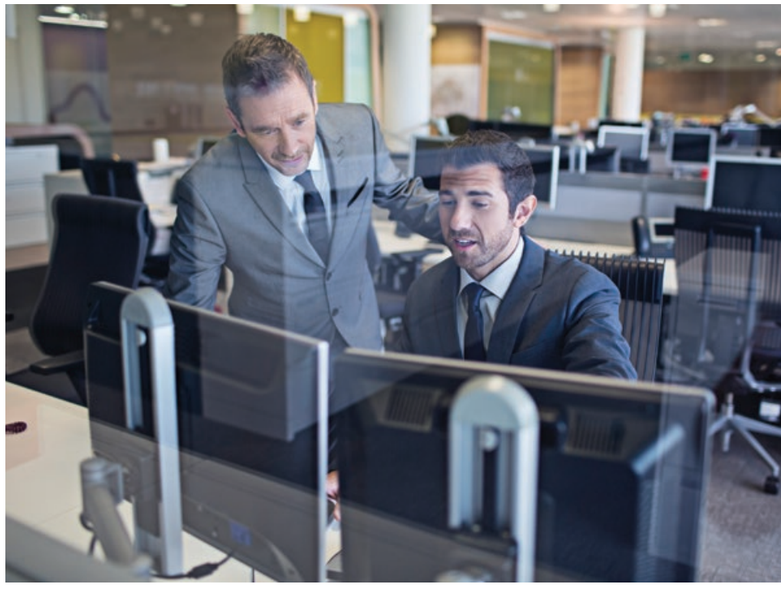
5

KOMUNIKÁCIA A PREVÁDZKA

Odporúčanie: V tejto fáze je dôležité transparentne a zrozumiteľne komunikovať dôležité zmeny pre ľudí v rámci vašej 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