

# 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 a agendy používajú univerzity 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 organizácie, s externými partnerskými organizáciami a ďalšími inštitúciami?
- Kto je zodpovedný za stratu osobných dát?
- Sú súčasné IT systémy a procesy v súlade s novým nariadením GDPR?
- Je univerzita pripravená na nové práva osôb? (právo na vymazanie, právo na prenos osobných údajov) v súlade s novým nariadením GDPR?

### DATALAN ako technologický partner za bezpečí:

- inventarizáciu informačných aktív
- kategorizáciu informačných aktív vrátane identifikácie väzieb informačných aktív na nariadenie o ochrane osobných údajov a príslušnú legislatívu

2

## IDENTIFIKÁCIA NEZHŔD

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 a súlad IT systémov s novým nariadením, ako napríklad prenos či vymazanie dát, ale aj nahlasovanie a riešenie bezpečnostných incidentov.

### DATALAN ako technologický partner za bezpečí:

- riziková analýza / 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 za bezpečí:

- 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 za bezpečí:

- Vykonanie zmien v existujúcich technológiách
- Obstarávanie a nasadenie riešení ako napríklad:
  - o riadenie a monitorovanie aktivít s osobnými údajmi
  - o archivácia záznamov
  - o pseudonymizácia a šifrovanie osobných údajov
  - o zabezpečenie dôveryhodnosti integrity, dostupnosti a odolnosti systémov spracovania 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 za bezpečí:

- proces pravidelného testovania prijatých opatrení a ich pravidelná aktualizácia

