
algotech

GDPR a kyberbezpečnost

12.5. 2025

Ondřej Krhůtek, Key Account Manager, Algotech

algotech

Agenda

- GDPR
- Kyberbezpečnost – NIS2

algotech

GDPR

algotech

GDPR – obecná fakta

Kdo spadá do GDPR?

Všechny právnické subjekty a organizace, které zpracovávají osobní údaje.

Platnost

Od 25.5. 2018 – neustále se aktualizuje a doplňuje (2024 – balanční test na kamery)

GDPR v kostce

OSOBNÍ ÚDAJ	Jakákoliv informace identifikující člověka
ZVLÁŠTNÍ KATEGORIE ÚDAJŮ	Velmi citlivé údaje (zdravotní stav, náboženství, sex. orientace)
ZPRACOVÁNÍ	Jakékoliv nakládání s osobními údaji: shromažďování, uložení, přístup, smazání, utřídění
SPRÁVCE	Určuje kdo, jak a proč zpracovává údaje
ZPRACOVATEL	Vykonává vůli správce
SUBJEKT ÚDAJŮ	Identifikovatelná osoba: zaměstnanec, zákazník, obchodní partner

algotech

GDPR v kostce – obecné principy

Zákonnost, korektnost a transparentnost

Zejména mít pro zpracování právní důvod (plnění právní povinnosti; plnění smlouvy; oprávněný zájem správce; souhlas se zpracováním apod.)

Účelové omezení

Minimalizace údajů

Uchovávej pouze ty OÚ, které skutečně potřebuješ pro daný účel

Přesnost

Průběžně aktualizuj zpracovávané OÚ; subjekt údajů má právo na opravu

Omezení uložení

Uchovávej pouze po dobu nezbytně nutnou – podle právního předpisu nebo vlastní určení.

Integrita a důvěrnost

Nastav vhodná technická a organizační opatření

Odpovědnost

Buď schopen doložit dodržování principů

algotech

Některá pravidla osvědčených postupů

Papírová podoba

- Systematická a přehledná správa dokumentů
- Pravidlo čistého stolu
- Průběžná skartace nepotřebných dokumentů
- Ukládání dokumentů do uzamykatelných úložných prostor (skříně, zásuvky)
- Konzistentní uzamykání skladovacích prostor

Elektronická podoba

- Používání a pravidelná rotace netriviálních hesel
- Soulad s vedením systému spisů a evidence dokumentů
- Pravidelné mazání nepotřebných nebo zastaralých souborů
- Třídění a pravidelné mazání e-mailů
- Zamkněte počítač, když odcházíte
- Odesílání osobních údajů pouze šifrované
- Omezit vzdálený přístup z veřejných Wi-Fi hotspotů
- Před otevřením přílohy věnujte pozornost celému e-mailu (předmětu, odesílateli, tělu)
- Nenavštěvovat neznámé nebo podezřelé odkazy v e-mailech nebo na webu

algotech

PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ (Data Breach)

- **Každý zaměstnanec**, který se dozví o porušení zabezpečení osobních údajů (data breach), **povinnost data breach neprodleně oznámit** (i) svému **nadřízenému a současně**
- Data breach mnoho podob = typicky ztráta, odcizení, poškození či zničení osobních údajů; př. ztráta či poškození databáze kontaktů; hackerský útok zvenčí, ztráta osobního PC či pracovního telefonu apod.
- *Oznámení subjektům údajů* + *Ohlášení ÚOOÚ* = pokud data breach představuje riziko pro práva a svobody fyzických osob

- **Pokud se zaměstnanec dozví o data breach nebo si není jistý, zda se jedná o data breach či nikoli, okamžitě kontaktovat svého nadřízeného (vedoucího oddělení) a odpovědnou osobu**
- Odpovědná osoba ohlásí ÚOOÚ **bez zbytečného odkladu a pokud možno do 72 hodin** od okamžiku, kdy byl závažný data breach reportován; **možnost ohlášení a jeho způsob bezodkladně konzultovat s externím odborníkem**
- Ohlášení ÚOOÚ má náležitosti dle GDPR

algotech

Kyberbezpečnost (NIS2)

algotech

NIS2 obecně

Co je NIS2?

NIS2 je aktualizovanou verzí směrnice NIS (Network and Information Security) z roku 2016. NIS2 výrazně rozšiřuje oblast působnosti platné legislativy a představuje nové řešení pro posílení a zabezpečení evropského kyberprostoru. **Členské státy EU mají za povinnost** tuto směrnici adaptovat do svého právního řádu.

algotech

NIS2 v kostce

Kdo spadá do NIS?

Kritéria:

1. nad 50 zaměstnanců nebo obrat nad 10 mio EUR
2. Provozování regulované služby (cca 105 služeb v 18 odvětvích)

Platnost

Směrnice v platnosti od října 2024, zákon zřejmě od 1.9. 2025

NIS2 a GDPR

- Většina kyberincidentů je zároveň únikem osobních dat
- Incidenty řeší oba úřady – NÚKIB a ÚOOÚ
- Opatření z GDPR lze částečně aplikovat v rámci NIS2

Proč s námi?

- **Komplexní služby** - audit, implementace, školení, testy, legislativa, zálohování, úložiště, tedy nejen navrhujeme opatření, ale je i technicky zrealizujeme
- **Pokrýváme celé portfolio služeb** z GDPR a kybernetické bezpečnosti
- **Vlastní SOC 24/7/365**
- **Česká společnost** - data ve vlastním datacentru, víme přesně kde jsou data uložena
- **Osobní přístup** k realizaci povinných opatření

algotech

Děkuji za pozornost

algotech


algotech