GDPR - General Data Protection Regulation

Nařízení Evropského parlamentu a Rady Evropské unie č. 2016/679 ze dne 27.4. 2016 (ve věstníku EU zveřejněno dne 4.5. 2016) . Účinnost nabude 25.5. 2018.

Základní terminologie
Subjekt údajů - fyzická osoba, o které jsou údaje zpracovávány
Správce - určuje účel a prostředky zpracování
Zpracovatel – ten kdo zpracovává osobní údaje na základě pokynů správce
Zpracování - jakákoliv operace s osobními údaji (uložení, změna, zaznamenání, výmaz, ..)
Pověřenec pro ochranu osobních údajů - Data Protection Officer (DPO), plní funkci koordinátora a kontaktní osoby pro správce, zpracovatele, subjekty údajů a úřady

Dotčené subjekty
Každá společnost či organizace, která zpracovává osobní údaje živých fyzických osob.

Zásady GDPR
GDPR není hrozba. Chápejme nařízení jako příležitost zajistit si data před únikem a následnými škodami.

1) Zákonnost, korektnost, transparentnost
2) Účelové omezení
3) Minimalizace sběru a zpracování údajů
4) Přesnost
5) Omezení při uložení
6) Integrita a důvěrnost
7) Princip odpovědnosti

Právní tituly zpracování
Každá operace s osobními údaji má být podchycena, v rámci směrnice o nakládání s osobními údaji, relevantním právním titulem. Titul si volí sám správce a za jeho oprávněnost a zákonnost nese důsledky.

- **Souhlas – používat co nejméně**
- **Plnění smlouvy**
- Plnění právní povinnosti
- Ochrana životně důležitých zájmů
- Plnění ve veřejném zájmu
- **Oprávněný zájem správce**

Souhlas
Jde v podstatě o zbytkový právní titul. Problém je v nadbytečnosti používání souhlasů. Co se stane po odebrání souhlasu? Jak bude souhlas zaznamenán, včetně informace o tom kdy a jak byl udělen?

- Souhlas u pracovních smluv
- Souhlas u dětí (aplikační právní norma počítá s věkem 13 let místo klasických 16 let)

Povinnost informovat
Správce by měl transparentně informovat o způsobu nakládání s osobními údaji.

- Totožnost a kontaktní údaje správce
- Jaké jsou účely zpracování
- Uvést příjemce nebo kategorie příjemců osobních údajů
- Informovat o právech subjektů
- V případě pověřence uvést kontakty na pověřence

Práva subjektů

1) Právo na informace
2) Právo na přístup k osobním údajům
3) Právo na opravu
4) Právo na výmaz
5) Oznamovací povinnost správce v případě hrubého selhání ohrožujícího subjekt
6) Právo na omezené zpracování
7) Právo vznést námitku
8) Právo na přenositelnost - pokud dochází ke zpracování údajů na základě smlouvy / souhlasu, a pokud se zpracování provádí automatizovaně, má subjekt právo získat údaje, které poskytl správci a které se ho týkají, ve strukturovaném, běžně používaném a strojově čitelném formátu, a má právo předat tyto údaje jinému správci. Nový správce ovšem nemusí tyto údaje přijmou.

Povinnost správce a právo na výmaz údajů

1) Dovršení účelu zpracování
2) Odvolání souhlasu
3) Protiprávní zpracování údajů

Vyjímky z povinnosti výmazu

1) Právo na svobodu projevu a informací
2) Právní povinnost zpracovávat osobní údaje
3) Veřejný zájem (zdraví, archivace)

Povinnost hlášení incidentů

1) Narušení bezpečnosti – do 72 hodin od chvíle kdy to správce/zpracovatel zjistí
2) Koho informovat
   * správce
   * ÚOOÚ
   * v případě závažného nebezpečí a ohrožení práva a svobody subjektu Subjekt
3) O čem informovat
   * povaha narušení + cca počet uniklých osobních údajů
   * kontakt na pověřence (DPO - Data Protection Officer)
   * pravděpodobné důsledky
   * popis opatření
4) Kdy není třeba informovat? Pokud není riziko

Projekt implementace

- Plán projektu
- Analýza aktivit a procesů
- Analýza stavu bezpečnosti (GAP analýza)
- Realizace implementace
- Ověření a kontrola

Implementace

- Odpovědná osoba – tým
- Outsorcing – vlastní zdroje
- Termíny

Analýza aktivit a procesů

- Osobní údaje a procesy práce s údaji
- Právní dokumenty
- Zabezpečení

Osobních údaje a procesy

1) Koho se OÚ týkají
2) Kde se OÚ získávají
3) Jaké OÚ se získávají
4) Účel zpracování
5) Právní titul
6) Citlivost a rizikovost
7) Kde se OÚ uchovávají
8) Forma uchování
9) Délka uchování
10) Zabezpečení
11) Osoby s přístupem
12) Komu se OÚ předávají
13) Reflexe práv subjektů

Právní dokumenty

- **Analýza právních dokumentů** (pracovní smlouvy, souhlasy se zpracováním OÚ, smlouvy se zákazníky, smlouvy o zpracování, smlouvy s IT, interní předpisy, obchodní podmínky)

- **Souhlasy se zpracováním** (nadbytečnost, zaznamenávání (kdy, jak) a archivace souhlasů, řešení v případě odvolání souhlasu, souhlas u dětí)

GAP analýza (rizikovost zpracování + zabezpečení, soulad rozsahu zpracování, soulad právních dokumentů, soulad právních titulů, soulad možností realizace práv + soulad procesů, DPIA-Data Protection Impact Assessment- posouzení vlivu na ochranu osobních údajů, DPO-Pověřenec)

Realizace implementace

- Omezení rozsahu údajů
- Zabezpečení
- Procesy
- Popis právních titulů
- Tvorba a úprava právních dokumentů
- Jmenování pověřence
- Školení zaměstnanců

Nejčastější slabá místa

1) Zpracování na základě doložených pokynů správce
2) Doba trvání, povaha zpracování, typ OÚ
3) Mlčenlivost
4) Technicko-organizační bezpečnostní opatření
5) Dodržování podmínek zapojení dalšího zpracovatele
6) Součinnost se správcem
7) Neproškolené osoby vstupující do kontaktu s OÚ

Martin Chudoba
TIXIK s.r.o.
tel.: **602 525 236**
e-mail: **mch@semtix.cz**

Příklad k řešení

Neziskovka z.s. - pořádá letní dětské tábory a soustředění pro děti.

Při objednání služby organizace požaduje tyto údaje:

- Jméno
- Příjmení
- Telefonní číslo
- Email
- Adresu
- PSČ
- Rodné číslo
- Datum narození
- Zdravotní pojišťovna
- Jméno zákonného zástupce
- Telefon na zákonného zástupce
- E-mail na zákonného zástupce
- Poznámka o zdravotním stavu

Při nástupu na tábor dále v nástupním listu uvádí

Dítě **je plavec** / **neplavec**
Dítě **má / nemá** úlevu z TV – jakou?
Dítě **má / nemá** alergii – na co?
Dítě **bere / nebere** pravidelně léky?
Další důležité informace …

Přihláška probíhá elektronicky přes internetové stránky organizace, může být odevzdána i v písemné podobě. Nástupní list se předává vytištěný v písemné podobě první den při nástupu na tábor.

Zákonní zástupci, kteří si chtějí nechat uhradit část ceny tábora od zaměstnavatele, mohou pořádat o vystavení faktury.

Veškerá ostatní komunikace probíhá elektronicky přes e-mail a telefon. Zákonný zástupce dostane po přihlášení emailový kontakt ke kterému mají přístup vedoucí tábora, a telefonní kontakty na vedoucí tábora. Kontakty na vedoucí jsou uvedeny i na webové stránce s přihlašováním.

Organizace dostává na pořádání táborů dotační příspěvek od města. Veškeré účetní operace realizuje hospodářka organizace s externí účetní kancelář, včetně vyúčtování dotací.

Data z přihlášek jsou uložené v cloudu u externí společnosti. K datům mají přístup všichni vedoucí tábora, kteří se účastní daného turnusu, zdravotnice, hospodářka, a IT zaměstnanci externí společnosti.

Věk a pohlaví přijatých dětí jsou uvedeny na webové stránce organizace, aby zákonní zástupci měli přehled o struktuře táborového kolektivu a vhodnosti pro jejich děti.

Data se uchovávají po dobu neurčitou. Na táboře se děti fotí, fotografie z každého dne, z konkrétních částí programu se pro informovanost rodičů dávají na Facebook.