

GDPR neboli General Data Protection Regulation je nově legislativní nařízení Evropské unie, platné od 25. května 2018

Troška teorie

Toto obecné nařízení představuje nový právní rámec ochrany osobních údajů v evropském prostoru, protože současná směrnice 95/46/ES již přestala odpovídat současné době.

Nařízení bude použitelné univerzálně v celé EU, tj. **bude platit stejně ve všech státech EU**. V českém právním prostředí nahradí doposud platný zákon č. 101/2000 Sb. o ochraně osobních údajů.

GDPR přináší nová pravidla pro všechny organizace, instituce a úřady v komerčním, neziskovém i státním sektoru, které nabízejí produkty a služby v Evropské unii nebo shromažďují a analyzují data obyvatel EU. Má za cíl hájit práva občanů proti zneužívání jejich osobních údajů.

Koho se týká:

- firem a organizací, které zpracovávají osobní údaje (pojem: správce nebo zpracovatel)
- jednotlivců, kteří poskytují osobní údaje (pojem: subjekt údajů) – zaměstnanec, zákazník fyzická osoba, majitel firmy, pacient, žák, student apod.

Nařízení se nevztahuje na fyzické osoby, které zpracovávají osobní údaje **výlučně pro osobní či domácí činnost**.

Osobní údaje jsou údaje o fyzické osobě (tzn. nejsou to údaje o firmách).

Patří sem:

- jméno, pohlaví, věk, datum narození, osobní stav, identifikační údaje vydané státem (např. rodné číslo), ale také IP adresa, telefonní číslo, e-mail či fotografický záznam
- plat, pracovní pozice, historie prohlížení internetových stránek

Zvláštní kategorií osobních údajů označované také jako „**citlivé**“ jsou:

- rasový či etnický původ, politické názory, náboženství, zdravotní stav, sexuální orientace, trestní delikty či pravomocná odsouzení
- genetické a biometrické údaje (např. otisk prstu), osobní údaje dětí

Zpracování citlivých údajů podléhá mnohem přísnějšímu režimu a větší ochraně než u běžných osobních údajů.

Osobní údaje nejsou:

- údaje o právnických osobách
- firemní e-mail např. obchod@firma.cz (ale personalizovaný firemní e-mail patřící právnické osobě již osobní údaj je, např. jméno.příjmení@firma.cz)
- údaje zemřelých osob a anonymizované údaje (tzn. bez možnosti určení konkrétní osoby, např. Petr z Brna)

Jak na to:

Pro splnění požadavků Nařízení bude nutné provést ve firmách celou řadu organizačních a technických opatření. Informační systém je jen jedna oblast, která s ochranou dat souvisí.

Práce na zavedení GDPR by tedy měla začít jinde, než v ekonomickém software. Základem je provedení analýzy vnitřního prostředí společnosti, posouzení rizik svých činností z pohledu ochrany osobních údajů a zmapování potřeby evidovaných osobních údajů (tj. zjištění právního titulu a účelu jejich zpracování) včetně provedení revize smluv a udělených souhlasů se zpracováním.

GDPR neudává konkrétní technologii na ochranu dat a k cíli zabezpečit data vedou různé cesty. V programu DUNA jsme se zaměřili na optimální postupy a provedení, nevolili jsme příliš nákladné techniky, jejichž výsledek by znamenal velkou investiční zátěž v porovnání s rizikem.

Pokladní software DUNA CASH je na GDPR připraven.

GDPR v software DUNA CASH

Novinkou v systému DUNA CASH je heslování ZIP souborů, které vznikají za účelem archivace dat. Tato nová funkce je volitelná a je možné ji zapnout nebo vypnout v *Nastavení* → *Nastavení GDPR* → parametr „Ano, chci“.

Nastavení GDPR

Pokud zvolíte ochranu dat z pohledu GDPR, tak při tvorbě ZIP souborů funkcí *Komprimace a archivace* a *Vytvoření bezpečnostní kopie* budou soubory chráněny heslem a bez tohoto hesla je nebude možné obnovit.

Heslo pro bezpečnostní kopie - se automaticky vygeneruje při startu programu, pokud ještě v *Nastavení GDPR* žádné neexistuje a jeho výchozí délka je nastavena na 12 znaků. Heslo je společné pro celou aplikaci, tj. všechny zpracovávané firmy. Uživatel může heslo změnit, zobrazit a vytisknout, přičemž jeho minimální délka musí být 4 znaky.

Zobrazení hesla se provádí kliknutím na ikonu , vytvoření nebo změna kliknutím na

ikonu  a tisk kliknutím na ikonu . Pokud při obnovování dat z bezpečnostní kopie bude heslo souhlasit se zde uloženým heslem, tak obnovení proběhne bez dalších dotazů.

Doporučujeme však **vytištění a uschování fyzického dokumentu s tímto heslem** pro případ záchrany dat z bezpečnostní kopie. Bez tohoto hesla nebude možné data obnovit v aplikaci, kde toto heslo není uloženo, a to ani výrobcem software, tj. firmou TILL CONSULT a.s., popř. jejími smluvními partnery.

Heslo pro uživatelské zálohy – je k dispozici pro vytváření ZIP souborů pomocí akce *Komprimace a archivace*. Lze zvolit přímo v *Nastavení GDPR* nebo je vyžadováno jeho zadání při první archivaci a následně se do konfigurace uloží pro opakované použití. Je možné jej změnit, zobrazit a vytisknout. Musí mít minimální délku 4 znaky a bude ve všech firmách stejné. Po kliknutí na ikonu  lze heslo zobrazit, na ikonu  lze heslo vytvořit nebo změnit a na ikonu  lze heslo vytisknout. Při dekomprimaci platí stejné pravidlo, jako u hesla pro bezpečnostní kopie – nebude vyžadováno, pokud bude souhlasit.



Nastavení pro GDPR

Nastavení napomáhající zabezpečení dat dle nařízení EU

Základní

Přejete si chránit data z pohledu GDPR?

☒ **Ano, chránit ***

- tato funkce vyžaduje v některých agendách zvýšená uživatelská práva.
- tato funkce zavádí šifrovací hesla, která budou chránit bezpečnostní kopie a uživatelské archivy ve formátu .ZIP.

Heslo pro bezpečnostní kopie *



Heslo pro uživatelské zálohy *



Toto heslo chrání zálohy vytvořené uživatelem 'Správce'

(*) Tato volba je společná pro všechny zpracovávané firmy



Jednorázové heslo

Toto heslo lze využít při vytváření ZIP soubor funkcí *Komprimace a archivace* v případě, pokud archivuje data pro někoho, komu není vhodné sdělovat soukromé uživatelské heslo. Toto heslo se nikam neukládá a je nutné ho sdělit uživateli, který bude dělat dekomprimaci popř. import dat ze ZIP souboru.

