GDPR neboli General Data Protection Regulation je nové legislativní nařízení Evropské unie, které vstupuje v platnost 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.

Ekonomický software DUNA je na GDPR připraven.

GDPR v software DUNA (od verze 2018-1-133)

Z důvodu větší ochrany dat jsou v software DUNA k dispozici některé nové funkce. Ale za připomenutí stojí i stávající funkce (např. propracovaná přístupová práva nebo vstup do programu pomocí hesel), které byly v souladu s požadavky GDPR již dnes.

Oblasti GDPR v software DUNA

- přístup do systému pomocí přihlašovacích hesel (stávající funkce)
- definování uživatelských práv pro práci v agendách (stávající funkce)
- heslování ZIP souborů, které vznikají za účelem archivace dat (nová funkce)
- žurnálování akcí s daty, prováděných konkrétními uživateli (nová funkce)
- uzamčení programu po delší době nečinnosti (nová funkce)

Uživatelé a jejich přihlašovací hesla

Všem oprávněným uživatelům doporučujeme přihlašování do programu pomocí individuálního hesla.

Přidání nového nebo zrušení stávajícího uživatele provádí Správce volbou *Agendy* → *Servisní akce* → *Komplet* → *Správce* → *Správa uživatelů*. Při jeho prvním přihlášení je pak vyžadováno vytvoření hesla, které by mělo být dostatečně „silné“ (o zapnutí silných hesel s určitými vlastnostmi se dozvíte v dalším textu). Další přihlášení daného uživatele je možné jen se zadaným heslem. Správce může ve zmíněné volbě heslo uživatele také vymazat, tj. nastavit na výchozí hodnotu „xxx“, pokud jej uživatel zapomene a postup vytvoření nového hesla se zopakuje. Pokud si chce svoje heslo vytvořit nebo změnit konkrétní uživatel, najde volbu pro změnu hesla v nabídce *Nastavení*.

Přihlašování uživatelů heslem je nezávislé na nastavení GDPR (viz text dále), ale v případě zapnutí zvýšené bezpečnosti, tj. parametr na záložce *Přihlašování*, to vylučuje možnost přihlašování pouze s heslem do systému (např. Windows) a přihlašování jako Správce bez hesla.

Přístupová práva pro práci v agendách

Jednotliví uživatelé programu mohou mít povolen přístup do různých agend odlišně. Úrovně přístupových práv jsou označeny číselně takto:

10 - přístup není povolen
20 - prohlížení údajů
30 - tisky, ukládání údajů do souboru (dbf, xls)
40 - nové zápisy
50 - oprava dnešních zápisů
55 - oprava zápisů z aktuálního měsíce
60 - oprava všech zápisů
70 - mazání
80 – přihrávání údajů ze souboru (dbf)
85 – tisky a exporty údajů do souboru v *Číselníku organizací* a *Personalistice* (GDPR)
90 - bez omezení

Čím vyšší právo, tím více možností práce s daty – to znamená, že určité právo vždy zahrnuje i činnosti dle nižších práv. Např. právo 60 umožňuje opravovat všechny záznamy, ale samozřejmě i vytvářet nové, což je obsaženo v nižším právu 40.

Nastavení práv uživatelů pro jednotlivé agendy provádí Správce ve volbě *Agendy* → *Servisní akce* → *Komplet* → *Správce* → *Správa uživatelů*.

V souvislosti s GDPR bylo zavedeno nové právo 85 pro tisk a exporty údajů do souboru, protože původní právo pro zmíněné operace 30 nesplňovalo požadavky na zvýšenou ochranu těchto dat.

Heslování ZIP souborů

Při komprimaci dat firmy za účelem jejich zálohování se využívají tři úrovně hesel:

- Heslo pro bezpečnostní kopie**,** které se samo vygeneruje a je jednotné pro všechny zpracovávané firmy v dané aplikaci. Je k dispozici pro Správce, popř. pro uživatele s právem dělat bezpečnostní kopie a s přístupem do *Nastavení základní konfigurace*, který jej může zobrazit a vytisknout, Správce navíc i změnit (viz *Nastavení GDPR*). Při běžné práci s bezpečnostními kopiemi se vždy použije uložené heslo, a pokud souhlasí, není uživatel obtěžován požadavkem na heslo. 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.

- Uživatelské heslo je k dispozici uživateli s právem vytvářet .ZIP soubor. 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 si jej zobrazit a vytisknout. Toto heslo se využívá pro všechny zpracovávané firmy pro konkrétního uživatele.

- Jednorázové heslo si vymyslí uživatel s právem vytvářet .ZIP soubor při archivaci 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.

Heslování souborů není volitelné a souvisí se základním parametrem pro GDPR. Pokud je zapnutý, tak se .ZIP soubory vždy chrání heslem.

Žurnálování akcí s daty

Program DUNA standardně uchovává historii operací s doklady a historii některých dalších akcí spuštěných uživatelem. Pro účely GDPR bylo sledování rozšířeno o určité operace s daty v evidencích, potencionálně obsahujících osobní údaje. Určitými operacemi se myslí tisky a exporty sestav, exporty dat do xls a dbf (u všech evidencí) a exporty e-mailových adres do schránky. Tyto aktivity uživatele může Správce vytisknout ve volbě *Servisní akce* → *Komplet* → menu *Správce* → sestava *Soupis provedených operací.* Rozšířené sledování uživatele je volitelné parametrem v *Nastavení GDPR* – záložka *Sledování.*

Uzamčení programu po delší době nečinnosti

Tato funkce slouží k ochraně dat v situaci, kdy není např. obsluha krátkodobě přítomna u počítače. Na základě zjišťování aktivity myši nebo klávesnice dojde po určité době nečinnosti k uzamčení aplikace. Otevřené evidence a zpracovávané doklady se skryjí

šedou plochou a další pokračování práce je možné po opětovném zadání přihlašovacího hesla uživatele. K zamykání nedochází v průběhu dávkových operací (např. komprimace a archivace dat, tvorba rozsáhlé tiskové sestavy). Časový interval, po jehož uplynutí dojde k uzamčení aplikace, zadává Správce v *Nastavení GDPR* → záložka *Zamykání* a tato doba je stejná pro všechny zpracovávané firmy.

! Výše uvedené funkce můžete využívat samostatně nebo vzájemně kombinovat. Jejich zapnutí a nakonfigurování parametrů proveďte ve volbě *Nastavení → Nastavení základní konfigurace → Nastavení GDPR.*

Nastavení GDPR

Záložka *Základní*

Zapnutý parametr „Ano, chránit“ ovlivňuje:

1. Chování programu při tvorbě ZIP souborů funkcí *Komprimace a archivace* a *Vytvoření bezpečnostní kopie* – soubory budou chráněny heslem a bez tohoto hesla je nebude možné obnovit.

2. Chování programu ve vybraných evidencích – v *Číselníku organizací* a agendě *Personalistika.* Protože tyto agendy obsahují osobní údaje, je potřeba pro funkce tisk a export zvýšit úroveň práva na 85.

Heslo pro bezpečnostní kopie - se automaticky vygeneruje při prvním startu programu, pokud ještě žádné neexistuje a jeho výchozí délka je nastavena na 12 znaků. Heslo je společné pro celou aplikaci, tj. všechny zpracovávané firmy. Je k dispozici pro Správce, popř. pro uživatele s právem dělat bezpečnostní kopie a s přístupem do *Nastavení základní konfigurace*. Uživatel může heslo zobrazit a vytisknout, Správce navíc i změnit, 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.

Heslo pro uživatelské zálohy – musí mít minimální délku 4 znaky a platí pro konkrétního přihlášeného uživatele a současně všechny firmy, tj. bude ve všech firmách stejné. Je k dispozici uživateli s právem dělat *Komprimaci a archivaci*. 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.

Záložka *Přihlašování*

Parametr na této záložce ovlivňuje přihlašování uživatele do programu. Při zapnutém parametru je vyloučena možnost přihlašovat se do programu bez hesla (automaticky se vypnou zapnuté parametry v *Aplikační konfiguraci „Postačuje přihlášení do systému“* nebo *„Přihlašovat se bez hesla jako správce“*) a síla přihlašovacího hesla se zvýší (délka hesla min 8 znaků, malá i velká písmena, numerický znak, speciální znak).

Pokud parametr na této záložce nebude zapnutý, lze sílu hesel i povinnost přihlašování s heslem nastavit samostatně v *Aplikační konfiguraci*.

Tento parametr nesouvisí se zapnutím parametru na záložce *Základní.*

Záložka *Zamykání*

Tento parametr umožňuje zamknout program DUNA po delší době nečinnosti. Dobu, po které se program zamkne, lze nastavit. Tento parametr nesouvisí se zapnutím parametru na záložce *Základní.*

Záložka *Sledování*

Parametr umožňuje shromažďovat informace o určitých operacích s daty v evidencích, potencionálně obsahujících osobní údaje. Určitými operacemi se myslí tisky a exporty sestav, exporty dat do xls a dbf (u všech evidencí) a exporty e-mailových adres do schránky.

Tento parametr nesouvisí se zapnutím parametru na záložce *Základní.*