



GDPR v KeISQL / KeIEXPRESS / KeIMINI / KeISTART

Úvodem

Od 25. 5. 2018 je účinné [nařízení EU 2016/679](#) o ochraně osobních údajů fyzických osob, zkráceně **GDPR** (pro zobrazení textu nařízení stiskněte na klávesnici Ctrl a klikněte myší na modrý text).

V tomto dokumentu jsou popsány funkce systému, které vám pomohou zpracovávat osobní údaje v souladu s nařízením (v závorkách jsou uváděna čísla příslušných článků nařízení). Dokument **předpokládá vaši nezbytnou znalost problematiky GDPR** a znalost stávajících funkcí systému – práce s číselníky, nastavení práv uživatelů, události a jiné. Pro podrobné informace o stávajících funkcích stiskněte v programu F1.

Funkce pro podporu GDPR jsou implementovány v modulu **Mzdy** a v číselnících, které obsahují nebo mohou obsahovat osobní údaje fyzických osob – **Osoby, Kontakty, Koneční odběratelé, Odběratelé a dodavatelé, Zákazníci e-shopu a Řidiči**:

- Omezení rozsahu evidovaných osobních údajů
- Kromě standardních přístupových práv také možnost nastavení práv uživatelů:
 - k tisku a exportu údajů z uvedených číselníků
 - k neplatným záznamům
 - k výmazu záznamů
 - k událostem GDPR.
- Evidence souhlasů se zpracováním osobních údajů a evidence žádostí subjektů o přístup, opravu, výmaz, omezení zpracování, odpovědí na žádosti apod.



Články 13 a 14 nařízení ukládají povinnost poskytovat subjektům údajů stanovené informace v okamžiku získání osobních údajů (a to i v případech, kdy není vyžadován souhlas subjektu se zpracováním). Tuto povinnost vám systém nijak nemůže usnadnit, neboť různé firmy poskytují různé informace podle oboru podnikání, účelu zpracování osobních údajů, svých oprávněných zájmů apod. Každá firma si tedy pro splnění této povinnosti musí vypracovat své dokumenty, které bude poskytovat subjektům údajů.

Omezení rozsahu evidovaných osobních údajů

Pokud jste to již neučinili, doporučujeme vám zkontrolovat, jaké osobní údaje v programu evidujete, kdo k nim má přístup, jak je zpracováváte, a zda k tomu máte zákonný důvod (viz článek 6 nařízení). I pouhé uložení v systému je dle GDPR zpracováním údajů (článek 4, odst. 2), a proto je **nezbytné omezit rozsah údajů jen na takové, které jsou evidovány v souladu s nařízením**.

Pro omezení rozsahu evidovaných údajů můžete využít následující funkce:



Skrytí nadbytečných polí

Aby uživatelé do systému nezadávali nadbytečné údaje, jejichž zpracování není v souladu s nařízením, můžete skryt pole, která nemají být plněna. V číselnících Osoby, Kontakty, Koneční odběratelé, Odběratelé a dodavatelé, Zákazníci e-shopu, Řidiči a v Seznamu zaměstnanců otevřete prohlížení libovolného záznamu  a stiskněte  Nastavit zobrazení polí. U jednotlivých polí (zejména u těch, která by mohla obsahovat osobní údaje) se zobrazí , po přepnutí do stavu se nebude dané pole zobrazovat při editaci záznamu.

Skrytím polí zamezíte jejich plnění, ale **nesmažete údaje**, které jsou v nich již obsaženy. Ke smazání nadbytečných údajů, které neevidujete v souladu s nařízením můžete použít následující funkci.

Hromadné smazání nadbytečných údajů

V číselnících Kontakty, Koneční odběratelé a Odběratelé a dodavatelé a můžete nadbytečné údaje smazat pomocí **exportu dat do Excelu**, smazání a následného **importu prázdných hodnot** (právo exportu/importu mají implicitně pouze správci, viz dále). Před touto akcí **doporučujeme zálohovat data** pro případ smazání nesprávných údajů.

V nástrojové liště číselníku stiskněte  a zvolte **Export/import kontaktů do Excelu** (nebo firem, konečných odběratelů). Pomocí tlačítka  přesuňte z levé části do pravé pole určená ke smazání a stiskněte **Export do Excelu**. V Excelu smažte nadbytečné údaje (nemažte záhlaví sloupců) a soubor uložte.


V okně *Export/import firem do Excelu* zapněte parametr **Importovat prázdné hodnoty**, stiskněte **Import z Excelu**, vyhledejte uložený soubor a potvrďte načtení.

Pro smazání nadbytečných údajů v jiných tabulkách systému kontaktujte programátory firmy KELOC CS.




Přístupová práva

Nastavením přístupových práv **zabezpečíte přístup ke zpracování osobních údajů pouze oprávněným osobám**. Kromě standardních přístupových práv k agendám, modulům, nabídkám, dokladům a číselníkům (viz nápověda F1 – Administrátor – Přístupová práva) jsou k dispozici také práva implementovaná speciálně pro účely GDPR. Všechna přístupová práva mohou nastavovat pouze správci.

Následující práva lze nastavit v číselnících Osoby, Kontakty, Koneční odběratelé, Odběratelé a dodavatelé, Zákazníci e-shopu a Řidiči v okně **Přístupová práva pro uzel/formulář**, které otevřete ve zvoleném číselníku ikonou  v pravém horním rohu.

Tisk/export údajů z číselníků

Pro zamezení neoprávněného tisku nebo exportu osobních údajů je **implicitně všem uživatelům** (kromě správců) **zakázáno tisknout a exportovat záznamy** z uvedených číselníků. Po stisku  nebo Výpis pro GDPR (viz dále) se zobrazí upozornění **Nemáte právo tisku/exportu**.

Pro povolení tisku/exportu oprávněným uživatelům se v okně *Přístupová práva pro uzel/formulář* v poli *Uzel* přepnete na **Tisk/export kontaktů** (nebo firem, konečných odběratelů, atd.) a oprávněným uživatelům nastavte **Přístup**.

Tisk obálek

Všichni uživatelé mohou tlačítkem **Tisk obálek** standardně vytisknout **pouze jednu obálku** označené firmy, konečného odběratele nebo kontaktu. Pro hromadný tisk více obálek je nutné povolit uživateli v daném číselníku přístup k tisku/exportu (viz výše).

Mazání položek v číselnících

Součástí GDPR je také ochrana osobních údajů před neoprávněným smazáním. Pro zamezení neoprávněného smazání osobních údajů je **implicitně všem uživatelům** (kromě správců) **zakázáno mazat položky** z uvedených číselníků.

Pro povolení mazání (firem, kontaktů, atd.) zapněte oprávněným uživatelům ve zvoleném číselníku v okně *Přístupová práva pro uzel/formulář* právo **Rušení**.

Neplatné záznamy

Podobně jako k platným záznamům je možné samostatně nastavovat i práva k neplatným záznamům číselníků (ukončení platnosti záznamů využijete např. při obdržení žádosti o omezení zpracování údajů, viz dále).

Pro nastavení práv k neplatným záznamům ve zvoleném číselníku se v okně *Přístupová práva pro uzel/formulář* v poli *Uzel* přepnete na **Neplatné záznamy** a uživatelům nastavte parametry **Prohlížení**, **Nový**, **Editace** a **Rušení**.


Další nastavení práv je k dispozici u událostí, které můžete využívat pro evidenci souhlasů, žádostí subjektů údajů a dalších úkonů souvisejících s GDPR (viz dále).

Přístupová práva dle typů událostí

V modulu CRM je v nabídce Nástroje volba **Přístupová práva dle typů událostí**. Uživatelům lze nastavit **Přístup**, **Zákaz** nebo **Prohlížení** u typů událostí, které budete využívat pro účely GDPR (viz dále).

Typy událostí GDPR

Typům událostí, které budete využívat pro účely GDPR, můžete v editaci nastavit specializaci GDPR (viz dále). Pro tyto typy událostí pak lze nastavit práva **Prohlížení**, **Nový**, **Editace** a **Rušení**.

Nastavení práv proveďte v modulu CRM v nabídce Doklady – Události. Otevřete *Přístupová práva pro uzel/formulář* ikonou  a v poli *Uzel* se přepnete na **Typy událostí GDPR**.

Mazání událostí

Implicitně je všem uživatelům (kromě správců) **zakázáno mazání událostí** běžných i událostí GDPR. Pro povolení mazání běžných událostí zapněte oprávněným uživatelům v modulu CRM v nabídce Doklady – Události v okně *Přístupová práva pro uzel/formulář* právo **Rušení**.

Nedoporučujeme povolovat mazání událostí GDPR (tj. událostí se zadaným typem události se specializací GDPR, viz dále). Např. smazání souhlasu subjektu se zpracováním osobních údajů evidovaného formou elektronické přílohy k události (viz dále) by mohlo mít za následek nezákonnost zpracování údajů.



Elektronické přílohy

Pokud budete evidovat souhlasy a žádosti subjektů údajů formou elektronických příloh k událostem GDPR (viz dále), je vhodné založit také speciální zařazení el. příloh pro GDPR a nastavit uživatelům požadovaná práva.

V modulu CRM je v nabídce Nástroje volba **Přístupová práva dle zařazení el. příloh**. Uživatelům lze nastavit **Přístup**, **Zákaz** nebo **Prohlížení**. Uživatelé, kterým nastavíte **Zákaz**, nebudou moci otevřít k náhledu elektronické přílohy daného zařazení.

Číselník **Zařazení el. příloh** otevřete tlačítkem přímo ze záložky El. přílohy – např. v editaci události nebo kontaktu. Jednotlivým el. přílohám v této záložce určete **Zařazení** výběrem z číselníku, nebo pole ponechte prázdné (u příloh, ke kterým nechcete nastavovat přístupová práva).

Evidence souhlasů a žádostí subjektů údajů

Obdržené souhlasy se zpracováním osobních údajů (článek 7), odvolání souhlasu, žádosti subjektů při uplatnění práv (články 15 až 21) i vaše odpovědi na žádosti a případná oznámení příjemcům (článek 19) lze evidovat **formou událostí s elektronickými přílohami**. Elektronickou přílohou události GDPR může být např. obdržený e-mail nebo naskenovaný dokument s podepsaným souhlasem nebo žádostí.

Přestože každý z číselníků má přímo v editaci položek záložku El. přílohy, ve které lze také evidovat souhlasy a žádosti, **doporučujeme k evidenci využívat události** mj. z následujících důvodů:

1. Pokud obdržíte žádost subjektu o výmaz (viz dále), vymazáním subjektu z číselníku ztratíte i přístup k jeho elektronickým přílohám. Naopak elektronické přílohy připojené u událostí zůstávají nadále dostupné (v modulu CRM), neboť **události subjektu v systému zůstávají i po výmazu subjektu**. Je to nezbytné kvůli prokázání zákonnosti zpracování osobních údajů při případné kontrole ÚOOÚ po dobu následujících 3 let. Po uplynutí této lhůty je možné vymazat i tyto události.
2. Událost GDPR lze zadat jako **úkol vybranému uživateli** včetně termínu splnění. Nesplněné úkoly se zobrazují daným uživatelům při spuštění modulu CRM nebo Mzdy. **Zobrazování nesplněných úkolů** při spuštění modulu aktivujete v nastavení modulu CRM v záložce Události a v nastavení modulu Mzdy v záložce Organizace.

Typy událostí GDPR

V modulu CRM – Číselníky – Typy událostí zadejte typy událostí, které budete používat pro účely GDPR – např. Souhlas se zpracováním osobních údajů, Žádost o přístup k osobním údajům, Žádost o výmaz apod. U každého typu události **nastavte specializaci GDPR** a pomocí parametrů určete, ve kterých číselnících se má daný typ událostí nabízet – např. Kontakty, Mzdy apod. Událostem GDPR také můžete zvolit barvu odlišnou od běžných událostí.

Zadání události

Při obdržení souhlasu nebo žádosti vyhledejte subjekt údajů v číselníku, ve kterém je evidován, klikněte na něj pravým tlačítkem myši a zvolte **Události**. Je-li subjektem údajů váš zaměstnanec, událost zadejte v seznamu zaměstnanců v modulu Mzdy.

V okně Události klikněte na , zadejte název a typ události, případně popis události, a v záložce El. přílohy připojte obdržený souhlas, odvolání souhlasu, žádost subjektu nebo vaši odpověď na žádost.

Jedná-li se o **žádost** např. o opravu údajů, můžete v události zapnout parametr **Úkol**, vybrat uživatele v poli **Řešitel** a stanovit **Termín splnění**. Úkoly se zobrazují řešiteli při spuštění modulu CRM nebo Mzdy (nastavení viz výše), dokud v editaci události nevyplní datum v poli **Splněno dne**.

Po vyřízení žádosti je možné také zaevidovat u subjektu **novou událost s informacemi o vyřízení žádosti** a s připojením příslušných dokumentů (nedoporučujeme však k událostem přikládat samotný Výpis pro GDPR).

Přehled událostí GDPR

Přehled všech událostí GDPR získáte v modulu CRM v nabídce Doklady – Události. Standardně se zobrazují všechny události systému, pro vyfiltrování událostí GDPR zapněte parametr **GDPR**. Vyfiltrovat lze také jeden vybraný typ události.

Nové události z tohoto místa zadávat nelze, **prohlížet a editovat události GDPR mohou pouze oprávnění uživatelé** (viz Přístupová práva).

Následující odstavce popisují, jakým způsobem v systému zpracujete žádosti subjektů údajů, které uplatní svá práva dle jednotlivých článků nařízení. Pro všechny žádosti společně platí, že je nejdříve zaevidujete jako událost GDPR k žádajícímu subjektu, a po vyřízení žádosti vyplníte v události datum v poli **Splněno dne** nebo zaevidujete novou událost s informacemi o vyřízení žádosti.



Právo na přístup k osobním údajům

Právo subjektu na přístup k osobním údajům (článek 15) může být realizováno formou poskytnutí výpisu údajů evidovaných v číselnících nebo v modulu Mzdy.

V editaci položek číselníků je k dispozici tlačítko **Výpis pro GDPR**. V jednoduchém textovém editoru zobrazí všechny údaje o subjektu evidované v dané položce číselníku – s možností tisku, uložení nebo zkopírování textu do jiného, předem připraveného dokumentu, určeného pro předání subjektu údajů.


Pro aktivaci tlačítka **povolte oprávněným uživatelům tisk/export údajů z číselníků** (viz Přístupová práva).

V modulu Mzdy je tlačítko Výpis pro GDPR aktivováno vždy, neboť osobní údaje evidované v tomto modulu jsou již dostatečně zabezpečeny samotným nastavením přístupu do modulu pouze oprávněným uživatelům (pokud mají do modulu Mzdy přístup i neoprávněni uživatelé, pak se jedná z hlediska GDPR o vážný problém).

V modulu Mzdy je tlačítko Výpis pro GDPR k dispozici:

- v editaci zaměstnanců
- v editaci pracovních poměrů
- v editaci dětí (v záložce Děti v editaci zaměstnanců i v nabídce Personalistika – Děti).

Právo na výmaz

Právo subjektu na výmaz („právo být zapomenut“, článek 17) realizujete **smazáním položky z příslušného číselníku** . Na dotaz jsou vymazány také veškeré údaje o subjektu z tabulky historie změn v číselníku.

Pro zamezení neoprávněného smazání osobních údajů je implicitně všem uživatelům (kromě správců) zakázáno mazat položky z uvedených číselníků (viz Přístupová práva).

Smazáním subjektu v číselníku **nedojde ke smazání dokladů**, ve kterých je subjekt uveden. Doklady je nutné uschovávat po dobu stanovenou příslušnými zákony (např. 10 let doklady rozhodné pro stanovení DPH).


Smazáním subjektu v číselníku také **nedojde ke smazání událostí GDPR**, které jsou nadále dostupné v modulu CRM. Např. obdržené souhlasy se zpracováním je nezbytné uschovávat ještě po dobu následujících 3 let kvůli prokázání zákonnosti zpracování osobních údajů při případné kontrole ÚOOÚ.

Právo na omezení zpracování

Právo subjektu na omezení zpracování (článek 18) může být realizováno **ukončením platnosti položky** číselníku, ve kterém je subjekt evidován. V editaci položky číselníku zadejte datum do pole **Platnost do**.

Neplatné položky číselníků se standardně nenabízí ke zpracování. Navíc je možné uživatelům nastavit speciální přístupová práva k neplatným položkám (viz Přístupová práva).

Právo na přenositelnost údajů

Právo na přenositelnost údajů (článek 20) můžete realizovat prostřednictvím exportu do Excelu , který je k dispozici v každém číselníku.

Bude-li pro tyto účely stanoven speciální formát, bude do systému implementován. V praxi se však tento článek nařízení bude uplatňovat spíše u velkých firem – finančních institucí, mobilních operátorů apod.