Návod

Nařízení GDPR
a program POHODA

STORMWARE POHODA
Ekonomický systém

www.pohoda.cz

Obsah

1. Úvod

Snad každý podnikatel nějakým způsobem nakládá s osobními údaji svých zákazníků, obchodních partnerů nebo třeba zaměstnanců. I proto se evropské nařízení dotýká tolika jednotlivců a firem. Ekonomický systém POHODA se na GDPR samozřejmě pilně chystá, pro uživatele bude plnit funkci nástroje, který zpracování osobních údajů umožní a co nejvíce usnadní.

V našem návodu si přiblížíme, co je podstatou nařízení GDPR, jak se na něj připravit a především na co nezapomenout. V jeho druhé části se pak dozvíte o správě údajů v ekonomickém systému POHODA v souladu s GDPR, možnostech zabezpečení dat a také o některých příkladech z praxe, díky kterým možná nejlépe pochopíte základní principy tohoto evropského nařízení. Na závěr vás čeká výběr otázek uživatelů programu POHODA na téma GDPR a našich odpovědí na ně – týkají se jak samotného programu, tak i správy osobních údajů obecně.

2. O evropském nařízení GDPR

Nařízení GDPR (General Data Protection Regulation) výrazným způsobem přepracovává legislativu o ochraně osobních údajů. Reaguje na současnou dobu, ve které se informační systémy a digitální podnikání obecně stávají nedílnou součástí téměř každé firmy. Dobu, v níž řada firem využívá ke komerčním účelům pojem big data nebo, lépe řečeno, sbírá informace, které po sobě zanecháváme v kyberprostoru.

Nařízení je jedním z nejrozsáhlejších právních předpisů, které Evropská unie v posledních letech přijala. Dokonce i skutečnost, že se nejedná o směrnici, ale přímo o nařízení, činí z GDPR neobvyklý právní předpis, který řada specialistů na ochranu údajů analyzuje a formou doprovodných pokynů dotváří. Bez nadsázky lze tedy říci, že se jedná o největší změnu legislativy v oblasti nakládání s osobními údaji za posledních 20 let.

GDPR se týká plošně všech firem, které spravují, shromažďují či zpracovávají osobní údaje občanů Evropské unie. V našem podnikatelském prostředí se tak bude jednat o všechny firmy a jednotlivce, kteří zpracovávají osobní údaje svých zaměstnanců, zákazníků nebo dodavatelů. GPDR se ale uplatní i na ty, kteří sledují a analyzují chování uživatelů na webu prostřednictvím nástrojů, jako je Google Analytics nebo Facebook. Cílem GDPR je totiž chránit digitální práva občanů EU.

2.1. Co je GDPR?

Nařízení GDPR nově reguluje zpracování osobních údajů fyzických osob, konkrétně upravuje ty oblasti, kde se dnes řídíme zákonem č. 101/2000 Sb., o ochraně osobních údajů. GDPR zavádí celou řadu nových práv a povinností a také zpřesňuje či zpřísňuje stávající pravidla.

2.2. Kdy bude GDPR platit?

Nařízení GDPR představuje právně závaznou normu, která vstoupila v platnost v květnu 2016 a musí být plně zavedena od 25. května 2018 v celém svém rozsahu ve všech státech EU.

3. Základní GDPR pojmy

Pro začátek je nejdůležitější porozumět základním GDPR pojmům – ostatně pak vám bude hned jasnější, jestli se vás GDPR vůbec týká.

Co všechno je osobní údaj?

Osobní údaj je jakákoliv informace o konkrétní fyzické osobě. Řekne-li se Jan Novák, ještě to není možno chápat jako osobní údaj – Janů Nováků je vícero. Pokud se ale tato informace spojí s dalším údajem, který už by identifikoval Jana Nováka jako konkrétní osobu (například adresa Palackého 1, Brno), pak už se jedná o osobní údaj. Kromě adresy, čísla a jiných identifikátorů to může být i jakýkoliv fyzický, fyziologický, genetický, psychický, ekonomický, kulturní nebo společenský rys této fyzické osoby.

Co jsou citlivé osobní údaje?

Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu než obecné údaje, protože mohou subjekty těchto údajů poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jejich diskriminaci. Jedná se o údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob.

Co se myslí zpracováním osobních údajů?

Zpracování osobních údajů je jakákoli operace, kdy je s údaji nějak manipulováno. Může to být například zaznamenávání, shromažďování, vyhledávání, nahlížení, přenos, ale i vymazání či zpřístupnění údajů, přičemž nezáleží na tom, jestli je to strojově nebo postaru – ručně. Zpracování zkrátka obsahuje všechny činnosti, při kterých je osobní údaj „přítomný".

Kdo je subjekt údajů?

Subjekt údajů je žijící fyzická osoba, které se osobní údaje týkají.

Kdo je správce osobních údajů?

Správcem je subjekt jakékoliv právní formy, který za zpracování primárně odpovídá. Určuje účely a prostředky zpracování osobních údajů.

Kdo je zpracovatel osobních údajů?

Zpracovatel osobních údajů je najímán správcem a jeho jménem zpracovává osobní údaje. Vždycky ale provádí jen takové operace, kterými ho správce pověří nebo jaké vyplývají z jeho dosavadní činnosti. Může se tedy jednat například o externí účetní, která pro podnikatele zpracovává osobní údaje jejich klientů.

Kdo je pověřenec pro ochranu osobních údajů?

Pověřenec pro ochranu osobních údajů (Data Protection Officer nebo zkráceně DPO) může být zaměstnancem vaší firmy nebo může úkoly plnit na základě smlouvy o poskytování služeb. Zároveň to může být právnická i fyzická osoba.

DPO v rámci vaší firmy poskytuje poradenství a informace o povinnostech podle GDPR, spolupracuje s dozorovým úřadem a působí jako kontaktní místo pro dozorový úřad. Nařízení GDPR přímo definuje, kdo takového pověřence potřebuje:

- úřad (státní správa) či veřejný subjekt,
- firma, jejíž hlavní činnost spočívá v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů (například zaměstnanců, klientů),
- firma, jejíž hlavní činnost spočívá v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

4. Jak se připravit na GDPR*

Příprava na GDPR může zabrat řádově i pár měsíců, a tak ji rozhodně nenechávejte na poslední chvíli. Pokud jste navíc větší firma, vyplatí se najmout si odbornou pomocnou ruku. Přece jen jde o rozsáhlé nařízení, se kterým se i odborníci teprve nedávno seznámili, a tak pravděpodobně nebude ve vašich silách vše svépomocí zvládnout.

Tato kapitola vám pomůže se v dané oblasti zorientovat – přehledně totiž uvidíte, co všechno musíte projít, zanalyzovat či upravit.

4.1. Interní audit

Hned na začátku si sesumírujte, jaké osobní údaje zpracováváte, jak a kdo s nimi nakládá a jak jsou zabezpečeny, také jak je archivujete, přenášíte nebo likvidujete. Zkrátka zhodnoťte aktuální stav ochrany osobních údajů ve vaší firmě a veškeré nedostatky vůči novým povinnostem, které vám GDPR ukládá. V tomto kroku si musíte zodpovědět například tyto otázky:

1. **Jaká zpracování provádím, zejména v personální a klientské agendě?**
   - Jsou osobní údaje zpracovávány manuálně, anebo automatizovaně?

2. **Proč a na základě jakého právního titulu osobní údaje zpracovávám?**
   - K plnění úkolů uložených zákonem? Např. vedení agendy sociálního zabezpečení.
   - K jiným účelům? Zejména plnění smlouvy, plnění podnikatelského záměru na základě souhlasu subjektu údajů, s využitím veřejných zdrojů, pro ochranu práv správce apod.
   - Splňuji požadavky pro zákonné zpracování?
   - Udal jsem dostatečný důvod pro zpracování osobních údajů?

3. **V jakém rozsahu se osobní údaje shromažďují?**
   - Provádím zpracování dat podle účelu, který jsem specifikoval?
   - Jsou shromážděná data adekvátní, přesná a účelná?

4. **V jakém termínu se osobní údaje likvidují?**
   - Uchovávám osobní data pouze po dobu nezbytně nutnou?

5. **Jakým způsobem se osobní údaje aktualizují?**
   - Jsou shromážděná data přesná a aktualizovaná dle potřeby?

6. **Komu mohou být osobní údaje zpřístupněny ve firmě nebo v rámci mých podnikatelských aktivit?**

7. **Mám stanovené interní normy týkající se zpracování osobních údajů?**

8. **Kdo je za dodržení interní normy týkající se výše uvedených bodů odpovědný?**

9. **Kdo je odpovědný za komunikaci se subjekty údajů?**
   - Mám k dispozici proceduru k určení práv subjektů dat s ohledem na jejich data, která zpracovávám?

10. **Chráním dostatečně osobní údaje?**
    - Zabraňují nasazené technické prostředky a uplatňovaná organizační opatření nahodilému přístupu k osobním údajům, jejich změně, zničení nebo ztrátě?

11. **Mám k těmto bodům vůbec nějakou dokumentaci?**
    (Pokud ne, založte si ji a veďte ji aktuální.)

* Zdroj: Sdružení pro internetový rozvoj, www.spir.cz

4.2. Interní systém

Nejlépe ve spolupráci s právníkem nastavte ve vaší firmě taková opatření, která budou odpovídat nárokům GDPR. Vycházejte přitom z provedeného interního auditu a zaměřte se mimo jiné na následující oblasti:

1. **Detailní přehled zpracování osobních údajů** ve vaší organizaci podle jednotlivých agend (např. personální, dodavatelská, odběratelská), který bude obsahovat následující části, resp. typy zpracování osobních údajů podle účelu zpracování:
   - Kategorie subjektů údajů, kterých se zpracování týká (např. klienti, potenciální klienti).
   - Právní tituly ke každému zpracování (např. se souhlasem subjektů údajů).
   - Délka zpracování osobních údajů v závislosti na účelu zpracování.
   - Uplatňování práv subjektů údajů (např. právo na přístup k osobním údajům).
   - Způsob archivace a následná likvidace osobních údajů.
   - Podmínky, za kterých jsou údaje předávány nebo zpřístupňovány třetím osobám.
     - Pokud ano, jak je nakládání s daty právně ošetřeno?
   - Popis jednotlivých informačních systémů zpracovávajících osobní údaje a jejich provázanost.
   - Seznam všech povinností ve vztahu k ochraně osobních údajů pro všechny v rámci celé firmy (bude se týkat například HR oddělení, marketingu, finančního a mzdového oddělení, supportu, client service, custumer care, back office, IT, vývoje produktu, výzkumu).
   - Zásady zabezpečení osobních údajů ve vztahu k příslušné agendě.

2. **Seznam všech stávajících povinností**

3. **Seznam odpovědností jednotlivých osob ve vztahu k povinnostem**

4. **Seznam všech úkolů**

4.3. IT systém

Když si pro správu osobních údajů zvolíte spolehlivý informační systém, máte z půlky vyhráno – umožní vám definovat role a přístupová práva uživatelů, sledovat jednotlivé agendy i typy zpracování údajů a spoustu dalšího. V rámci příprav na GDPR vám zkrátka mnohé usnadní:

- načítat data z aplikací a ta dále dle nastavených procesů zpracovat,
- definovat reporty a procesy na základě rolí, skupin a organizační struktury,
- veškeré dokumenty lze archivovat a opatřovat elektronickým podpisem,
- k dokumentům lze na konci procesu vytvářet souhrnnou zprávu,
- definovat role, skupiny, organizační strukturu,
- v rámci číselníků lze sledovat jednotlivé agendy i typy zpracování,
- případně data regulátorovi odesílat přímo datovou schránkou.

TIP *S čím vám pomůže ekonomický systém POHODA, se dozvíte v následujících kapitolách.*

4.4. Seznam nových povinností

V tomto kroku byste už měli mít v ruce všechny dokumenty, které analyzují aktuální stav nakládání s osobními údaji ve vaší firmě. Teď je čas na to, abyste je porovnali s tím, co po vás žádá GDPR.

Posouzení vlivu na ochranu osobních údajů

Nařízení GDPR (konkrétně článek 35) mluví o tzv. Data Protection Impact Assessment (DPIA), což je nástroj, který pomáhá organizacím posoudit vliv na ochranu osobních údajů a identifikovat nejefektivnější způsob, jakým uvést interní pravidla do souladu s GDPR. Vy tak musíte vyhodnotit, zda máte povinnost DPIA dokumentaci vypracovat.

- DPIA se povinně provádí:
  - při systematickém a rozsáhlém vyhodnocování osobních aspektů týkajících se fyzických osob, které je založené na automatizovaném zpracování (včetně profilování),
  - při rozsáhlém zpracování citlivých osobních údajů,
  - při rozsáhlém systematickém monitorování veřejně přístupných prostorů,
  - další případy, kdy je provedení DPIA povinné, může určit dozorový orgán.

- DPIA musí obsahovat alespoň:
  - popis zamýšleného zpracování, účel a oprávněné zájmy,
  - posouzení nezbytnosti a přiměřenosti zpracování,
  - posouzení rizik pro práva a svobody subjektů údajů,
  - plánovaná opatření k odstranění nebo snížení těchto rizik.

Z výsledků analýzy DPIA může vyplynout, že některá rizika nelze eliminovat nebo je snížit. V případě kontroly dozorového úřadu tak budete moci vše potřebné doložit, právě díky této dokumentaci.

Získání souhlasu se zpracováním osobních údajů

Není pravda, že pro každé zpracování osobního údaje je potřeba souhlas. Nepotřebujete jej a ani byste ho po subjektu údajů neměli vyžadovat v případech, kdy:

- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,

- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,

- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,

- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,

- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů,

Pokud zpracováváte údaje z jiných než výše uvedených důvodů, souhlas už prokázat musíte. Musí být tedy zaznamenán prokazatelně a musí být v případě potřeby doložitelný, v tomto ohledu není problém ho mít e-mailem. Dále souhlas musí být dobrovolný, nelze jím podmínit čerpání nějaké služby. Musí být také jednoznačný v účelu a rozsahu, musí být oddělený například od obchodních podmínek, nesmí být schovaný ve smlouvách apod. Také musí být konkrétně stanoveno, za jakým účelem je poskytnut, například za účelem zasílání obchodních sdělení. A v neposlední řadě musí být souhlas informovaný, tj. musí být jasné, komu je souhlas udělen, že se nepředává mimo EU a jak je možné jej odvolat.

Pověřenec pro ochranu osobních údajů

Úlohu pověřence pro ochranu osobních údajů jsme si vysvětlili už v rámci základních GDPR pojmů. Proto jen připomínáme, že některé firmy či organizace takovou osobu jsou povinni mít.

Revize interních pravidel i uzavřených smluv

Spoustu osobních údajů spravujete na základě smluvního vztahu, zrevidujte či aktualizujte veškeré dodavatelské smlouvy. Nezapomeňte ani na své zaměstnance – poučte je o zásadách GDPR a proškolte je v nastavených interních pravidlech.

Práva subjektu údajů

Právo na opravu
Každý subjekt má podle nařízení GDPR právo požádat o opravu nepřesných údajů, které o něm evidujete.

Právo na výmaz
Subjekt údajů má právo na vymazání svých osobních údajů ze strany správce, je-li dán jeden z nařízením vyjmenovaných důvodů, mezi které patří:

- Osobní údaje již nejsou potřebné pro účely, pro které byly zpracovány.
- Subjekt údajů odvolal svůj souhlas se zpracováním.
- Osobní údaje byly zpracovány protiprávně.

Právo na omezení zpracování
Správce je povinen omezit zpracování v případech, kdy:

- subjekt údajů popírá správnost svých osobních údajů. Po dobu, kdy bude správce údajů ověřovat přesnost a správnost osobních údajů subjektu, má subjekt údajů právo, požádat správce o omezení použití těchto nepřesných dat;
- zpracování osobních údajů je protiprávní, ale subjekt údajů nepožaduje jejich výmaz, ale pouze požaduje omezení zpracování těchto dat;
- správce osobní údaje již nepotřebuje pro účely zpracování (a měl by je tak smazat), ale subjekt údajů je požaduje z důvodu určení, výkonu nebo obhajoby právních nároků;
- subjekt údajů podal námitku proti zpracování. Po dobu, kdy bude ověřováno, zda převažují zájmy správce či subjektu, je nutné omezit zpracování těchto dat.

4.5. Analýza rizik

Pokud jste správně provedli všechny přechozí kroky, máte k dispozici potřebné podklady pro vyhodnocení rizikových oblastí. Tato analýza by měla obsahovat alespoň následující prvky:

1. **Popis posuzované aktivity** – definice, účel, charakteristika
2. **Klasifikace rizika (nízké/střední/vysoké)**
   - Vysoké riziko zakládá např. povinnost provést hodnocení dopadů na ochranu osobních údajů (DPIA, dle článku 35 GDPR) nebo povinnost předchozí konzultace s dozorovým úřadem (dle článku 36 GDPR).
   - Vysoce rizikovým je např. zpracování, které využívá nových technologií a kde je pro subjekt údajů obtížné uplatnit svá práva.
   - Nízké riziko naopak připouští některé výjimky z povinností, např. z povinnosti ohlašovat porušení zabezpečení dozorovému úřadu (dle článku 33 GDPR).
3. **Pravděpodobnost vzniku škody**
   - Pravděpodobnost stoupá např. s počtem osob zapojených do zpracování osobních údajů a se zapojením třetích stran, pravděpodobnost může zvýšit také historie předchozích incidentů, kdy ke vzniku škody došlo.
4. **Klasifikace možné škody (malá/střední/velká)**
   - Závažnost možné škody je dána zejména mírou citlivosti údajů, objemem zpracovaných osobních údajů, mírou zranitelnosti dotyčné osoby nebo mírou dopadu na ekonomické a společenské poměry dotyčné osoby.
5. **Typizace škody**
   - Materiální (např. škoda na majetku zneužitím platebních údajů)
   - Nemateriální (např. poškození dobrého jména, zneužití identity)
   - Společenská (např. diskriminace)
6. **Identifikace případného sektorově-specifického rizika**
   - Hodnocení vztahu rizika a přínosu zpracování osobních údajů
   - Přínos organizaci (např. možnost implementovat řešení)
   - Přínos společnosti (např. veřejný zájem)
   - Přínos jednotlivci (např. možnost čerpat požadovanou službu)
7. **Posouzení případných globálních souvislostí v případě nadnárodních společností**

4.6. Opatření k odstranění rizik

Posledním krokem jsou opatření, která ve firmě nastavíte, abyste všem rizikům z provedené analýzy předešli nebo je odstranili.

Opatření k odstranění rizik mohou například spočívat v následujících činnostech:

1. Zaměstnanci budou proškoleni o GDPR a s ním souvisejících nových povinnostech (například povinnost doložit souhlas subjektu údajů se zpracováním osobních údajů). Účast na školení bude dokladována a/nebo se zaměstnanci podpisem zavážou dodržovat interní pravidla týkající se ochrany osobních údajů.

2. Omezíte počet osob, které mají k osobním údajům přístup, na ty zaměstnance, kteří s daty skutečně pracovat musí. O smluvních partnerech a dalších stranách nemluvě.

3. Přístup k osobním údajům bude zabezpečen i fyzicky či technicky. Už žádné počítače bez hesla, hesla nalepená na monitorech, volné přenášení osobních údajů na jakémkoliv nosiči ven z firmy nebo odemčená volně přístupná kartotéka, ani ukládání dokumentů obsahujících osobní údaje na nezajištěných veřejných online úložištích.

4. IT oddělení nebo správce IT sítě upraví bezpečnostní procesy tak, aby minimalizovaly možnosti úniku osobních údajů.

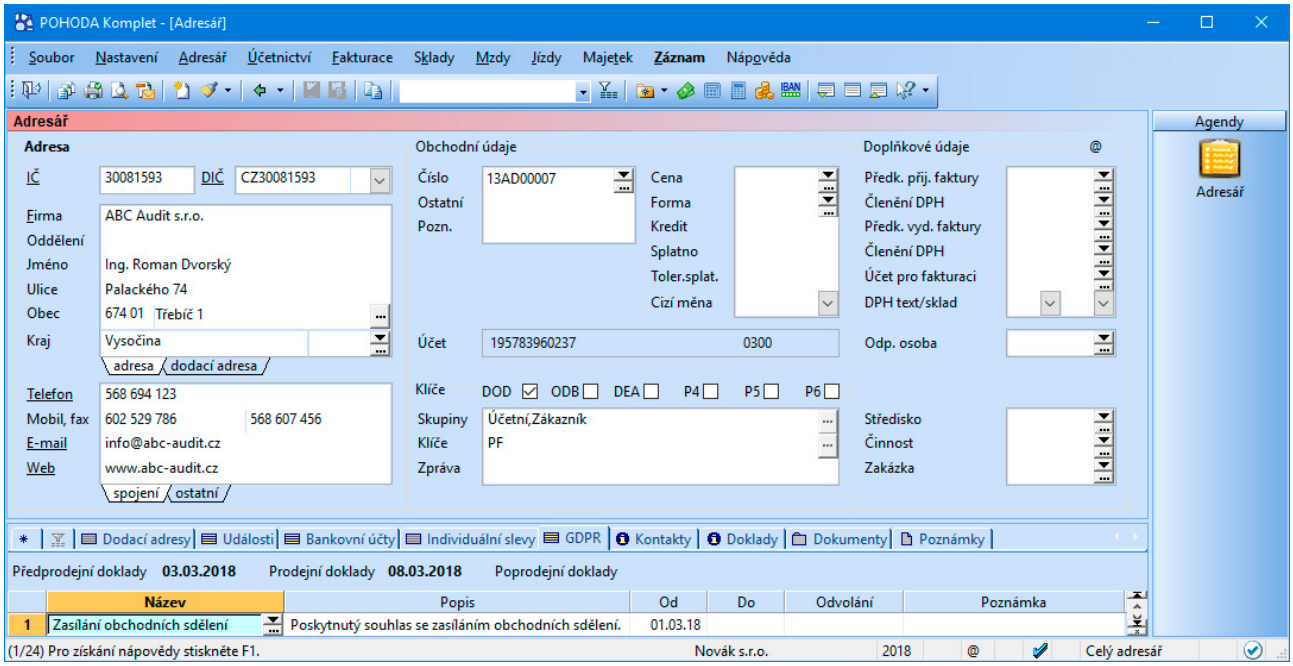
5. Zlikvidujete osobní údaje, pro jejichž uchovávání již neexistuje oprávněný důvod.

6. Data, která lze anonymizovat, anonymizujete.

5. Správa osobních údajů v programu POHODA

Pro správu osobních údajů v programu POHODA je nejvhodnější agenda Adresář. Jelikož do ní už v základu ukládáte veškeré kontaktní a fakturační údaje zákazníků či dodavatelů, je ideální, když budete na stejném místě spravovat i vše potřebné dle nařízení GDPR. Konkrétně odkdy, dokdy a proč máte údaje v evidenci, jak se účel jejich zpracování časem měnil nebo třeba kdo s údaji pracuje. Funkčnost pro GDPR je potřeba nejprve aktivovat v agendě Globální nastavení/GDPR zatržením volby Povolit GDPR.

V agendě Adresář se zpřístupní záložka GDPR, na které si jednoduše vyberete účel zpracování údaje ve sloupci Název, podle kterého POHODA automaticky doplní popis důvodu, a potřebná data zpracování údaje. POHODA vám důvody zpracování sama nabídne, do seznamu si ale samozřejmě můžete přidat i vlastní. Jak na to, se dozvíte hned v následující kapitole.



Záložka GDPR v agendě Adresář skrývá ještě jednu užitečnou funkci z pohledu správy osobních údajů. Řekne vám totiž, kdy naposled jste danou adresu použili na předprodejních, prodejních a poprodejních dokladech:

Předprodejní doklady – Přijaté nabídky, Vydané nabídky, Přijaté poptávky, Vydané poptávky

Prodejní doklady – Banka, Pokladna, Interní doklady, Přijaté objednávky, Vydané objednávky, Vydané faktury, Vydané zálohové faktury, Ostatní pohledávky, Přijaté faktury, Přijaté zálohové faktury, Ostatní závazky, Prodejky

Poprodejní doklady – Reklamace, Servis

Z pohledu nařízení GDPR se tak vyplatí vše (počínaje vydanou nabídkou a reklamačním protokolem konče) evidovat přímo v ekonomickém systému POHODA, jedině tak budete mít dokonalý přehled o zpracování osobních údajů. Dobu, po kterou je pro vás vystavení jednotlivých typů dokladů důvodem pro zpracování osobních údajů obchodních partnerů, si můžete nastavit v agendě Globální nastavení/GDPR.

5.1. Vyhledání, úprava a vymazání osobních údajů

Každý subjekt má podle nařízení GDPR právo požádat o opravu nebo vymazání údajů, které o něm evidujete. Díky programu POHODA údaje rychle vyhledáte, upravíte, ale i vymažete.

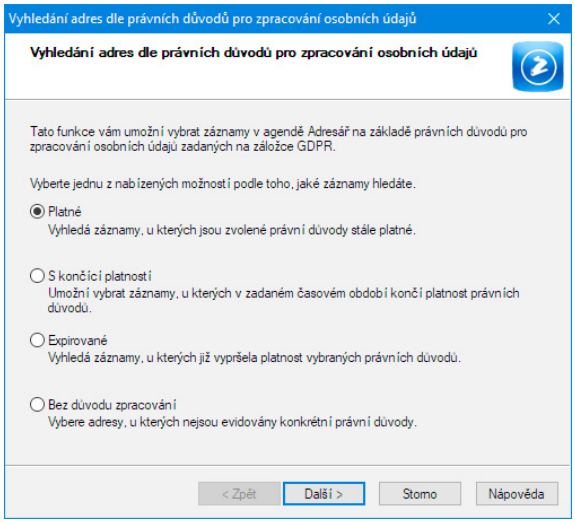
TIP *Práci se záznamy se věnuje 7. díl e-learningového kurzu POHODA – školení základních dovedností.*

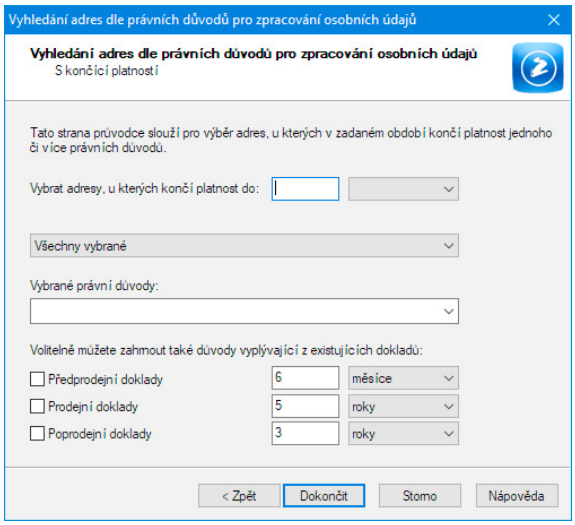
Pod nabídkou Záznam/GDPR agendy Adresář navíc najdete vychytávky pro hromadné vyplnění záložky GDPR u více adres najednou (povel Hromadně přidat důvod zpracování…) a pro výběr adres s aktuálně platným souhlasem či účelem nebo naopak s končícím souhlasem k určitému datu (povel Vyhledat záznamy…). Možností vyhledávání adres podle právních důvodů zpracování je hned několik, POHODA rozlišuje:

1. Platné důvody
2. Důvody s končící platností
3. Expirované důvody
4. Adresy bez důvodu zpracování

Podle zvolené možnosti se na druhé straně průvodce zobrazí rozšířené volby pro vyhledávání. V případě bodu 1–3 lze vyhledat:

- **Všechny důvody** – POHODA vybere adresy, u kterých je zadaný alespoň jeden právní důvod, a zároveň jsou všechny zadané důvody platné.
- **Jakýkoliv důvod** – POHODA vyhledá adresy, u kterých existuje alespoň jeden právní důvod, který je zároveň platný.
- **Některý z vybraných** – POHODA umožní v dalším poli pomocí výklopného seznamu vybrat konkrétní právní důvody. Následně vyhledá adresy, u kterých je alespoň jeden z těchto vybraných důvodů platný.
- **Všechny vybrané** – tato možnost je podobná jako u předchozí volby, tentokrát však musí být u záznamu všechny vybrané důvody vyplněné a všechny musí být platné.



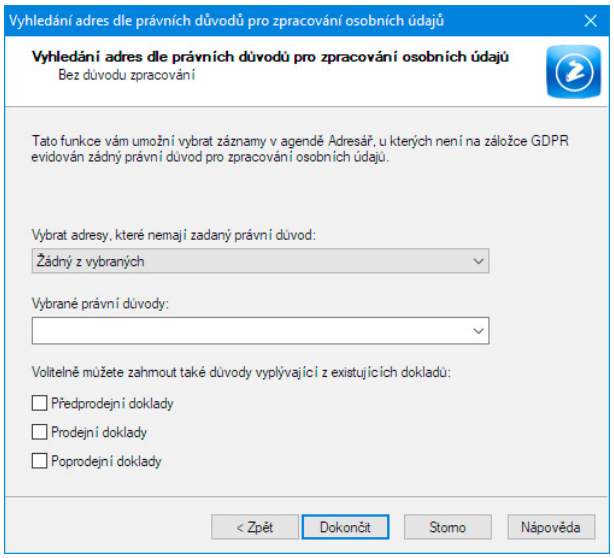


Rozdíl mezi volbami Všechny a Všechny vybrané spočívá mimo jiné v tom, že volba Všechny zohledňuje pouze důvody u adresy skutečně zadané. Oproti tomu při volbě Všechny vybrané se požaduje, aby adresa skutečně obsahovala všechny vybrané důvody, jinak do filtru nevstoupí.

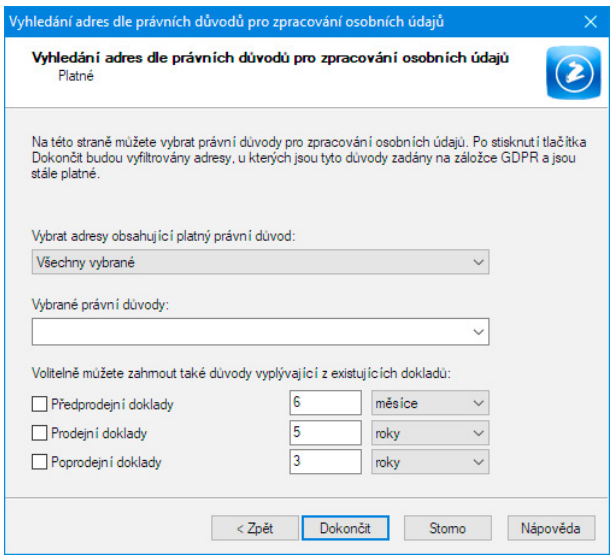
*Pouze v případě hledání expirovaných adres máte k dispozici volbu **Včetně adres bez vyplněného důvodu**. Pokud tedy u adresy není zadaný důvod, bere se adresa pro účely hledání stejně, jako by byl důvod expirovaný.*

V případě poslední možnosti, tedy adres bez důvodu zpracování, lze vyhledat:

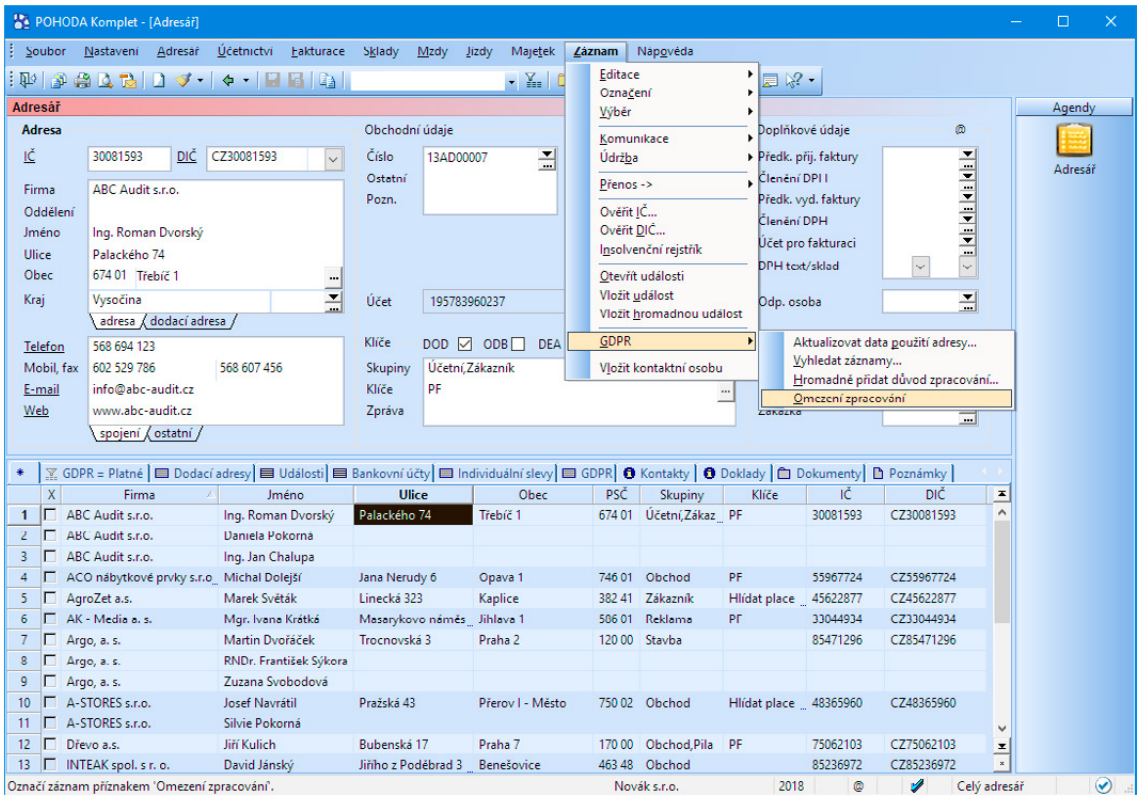
- **Žádný důvod** – POHODA vybere adresy, u kterých není zadaný žádný důvod zpracování.
- **Některý z vybraných důvodů** – POHODA vyhledá adresy, u kterých chybí alespoň jeden z vybraných důvodů.
- **Žádný z vybraných důvodů** – POHODA vyhledá adresy, u kterých není ani jeden z vybraných důvodů.



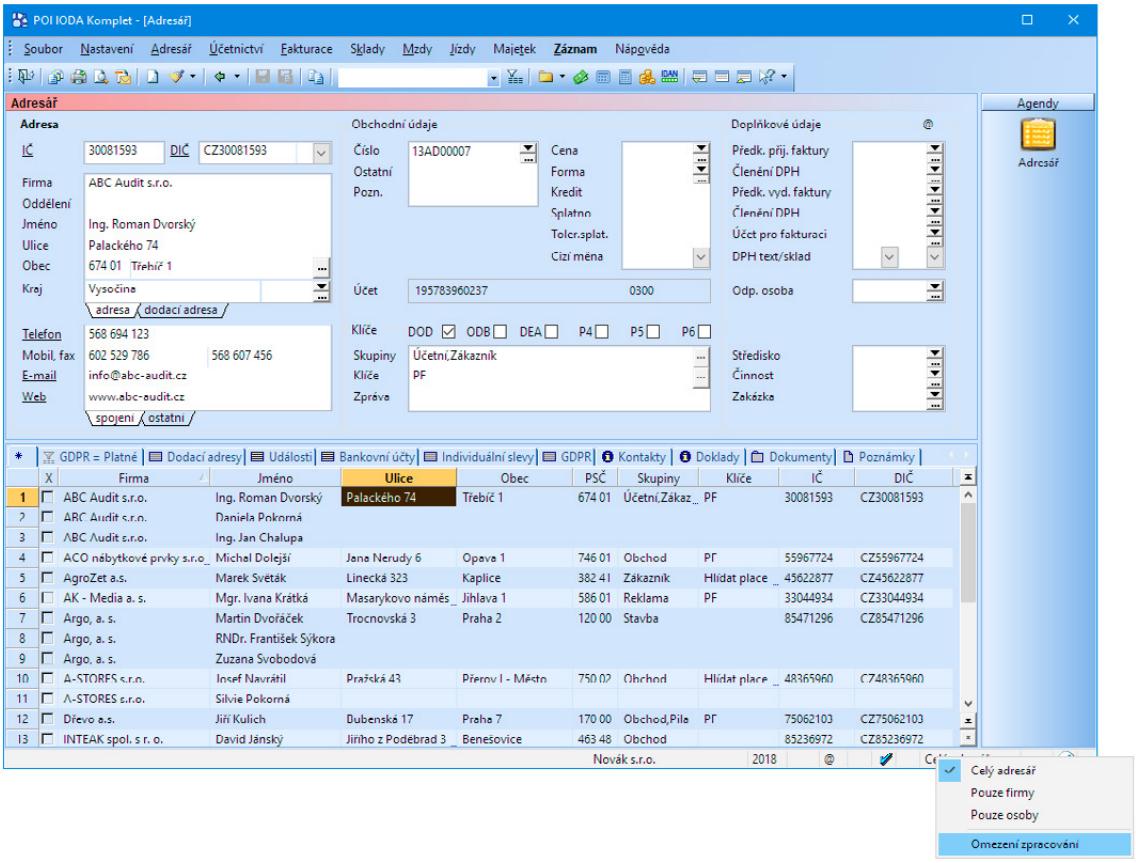
Ve všech možnostech vyhledávání (1–4) pak můžete volitelně zahrnout také důvody vyplývající z vystavených dokladů – předprodejních, prodejních a poprodejních.



POHODA vám umožní také konkrétní adresu označit příznakem Omezení zpracování, který zajistí, aby adresa nebyla pro uživatele programu viditelná, a znepřístupní ji tak pro další použití. Jde o umožnění realizace práva subjektu na omezení zpracování dle článku 18 Obecného nařízení o ochraně osobních údajů.

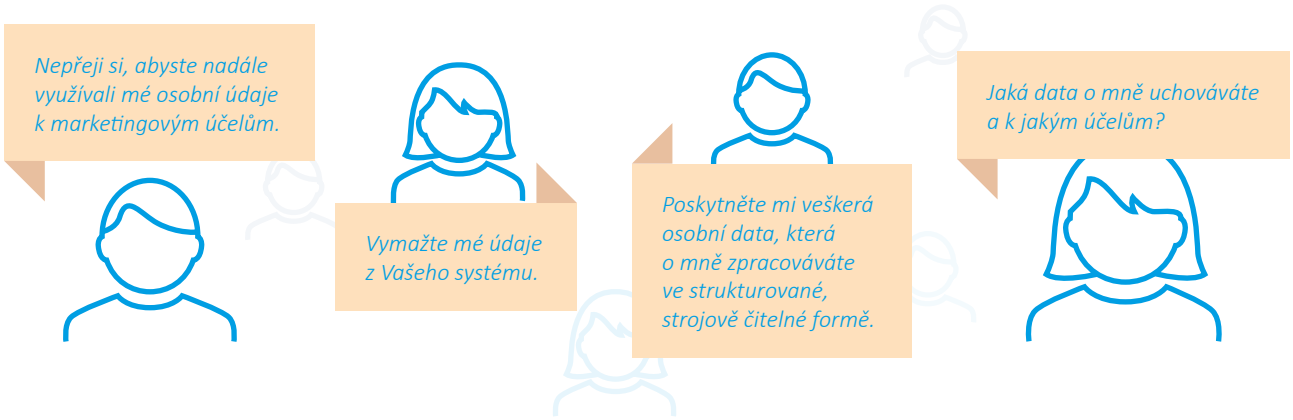


Všechny adresy, kterým jste přiřadili příznak Omezení zpracování, si zobrazíte pouhým kliknutím pravého tlačítka myši na stavový řádek v části, kde se volí rozsah zobrazení záznamů, a zvolením možnosti Omezení zpracování.



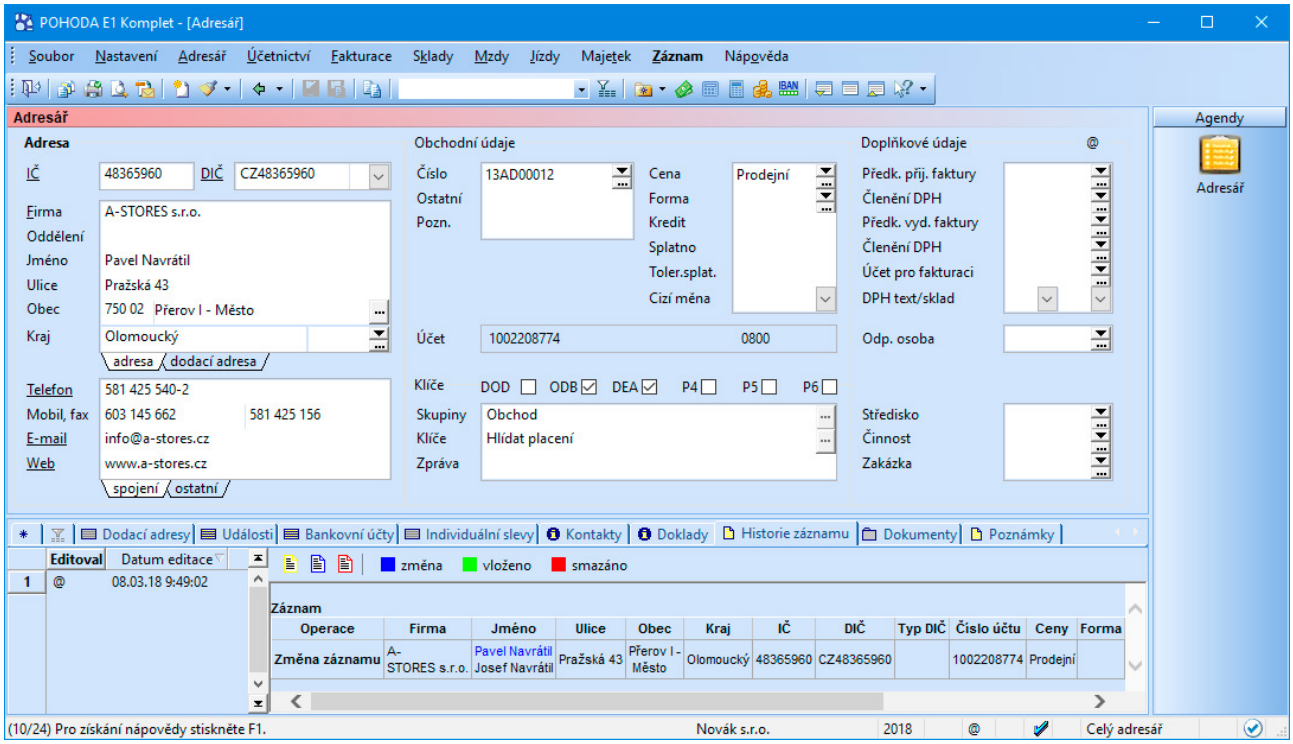
S programem POHODA tak budete vždy schopni reagovat na požadavky subjektů údajů:

- Vymažte mé údaje z vašeho systému.
- Poskytněte mi veškerá osobní data, která o mně zpracováváte ve strukturované, strojově čitelné formě.
- Nepřeji si, abyste nadále využívali mé osobní údaje k marketingovým účelům.
- Jaká data o mně uchováváte a k jakým účelům?



5.2. Historie změn údajů

Jednoduše zkontrolujete, kdy a kdo z uživatelů programu s údaji manipuloval. Pokud dojde k opravě údaje, POHODA uloží jeho původní verzi automaticky na záložku Historie záznamu. Smazané, změněné a nově vložené údaje jsou na záložce pro lepší přehled barevně označeny.

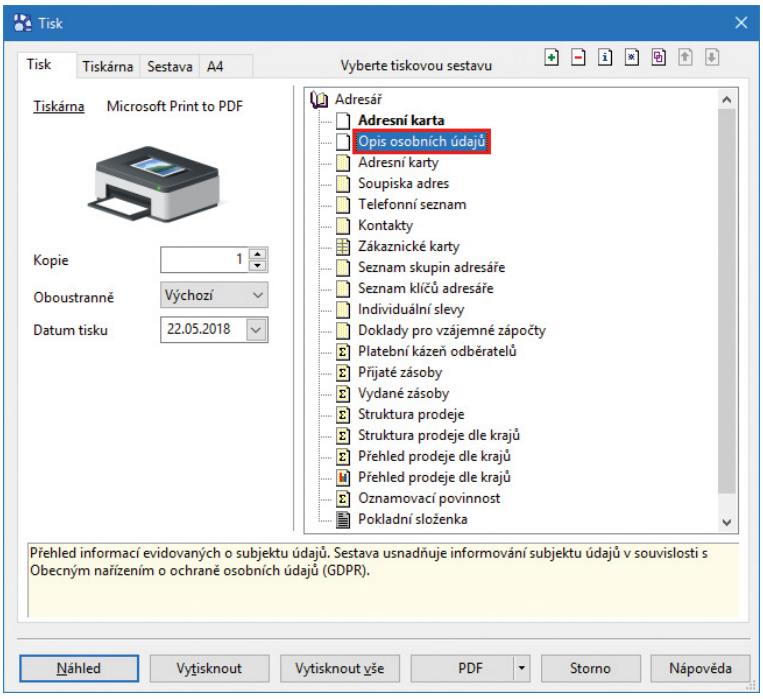


Historii změn v jednotlivých agendách si jednoduše zapnete v agendě Globální nastavení, a to prostřednictvím volby Evidovat historii změn. Tato funkčnost je pro většinu agend dostupná ve všech řadách programu POHODA, pro účely GDPR ji využijete jak v agendě Adresář, tak Personalistika.

5.3. Soupiska s údaji vybraného subjektu

Pokud vás někdo požádá o předložení uceleného souhrnu jeho osobních dat, jednoduše si vygenerujte tiskovou sestavu Opis osobních údajů přímo z agendy Adresář, která vám tento soupis poskytne (sestava se zpracovávanými údaji se vám zajisté bude hodit také při případné kontrole). S programem POHODA tak budete vždy schopni reagovat na práva subjektů údajů dle článku 15 nařízení GDPR.

Je-li ve vaší organizaci jmenován pověřenec pro ochranu osobních údajů, můžete údaje o něm zadat v agendě Globální nastavení/GDPR, čímž se budou tisknout na sestavě Opis osobních údajů.



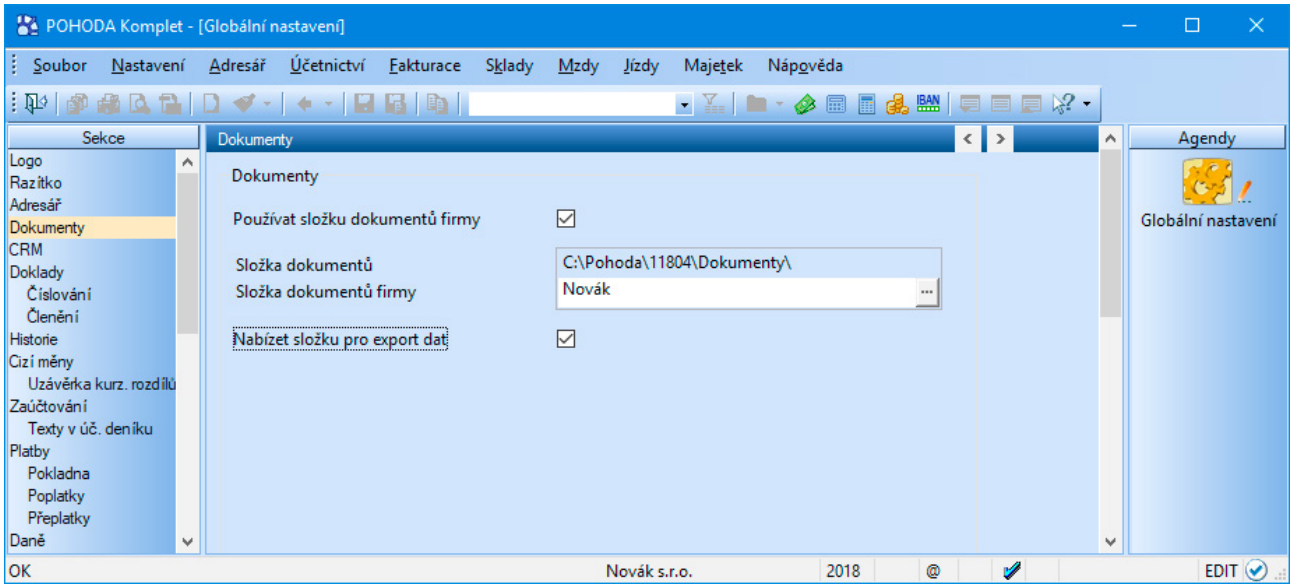
5.4. Práce s dokumenty

Všechny své dopisy, smlouvy, tabulky a jakékoli další důležité dokumenty si můžete v programu POHODA přehledně uspořádat. Snadno je přiřadíte k adresám i k událostem a přistupovat k nim můžete nejen z programu Průzkumník v Microsoft Windows, ale také z vybraných agend. Z hlediska nařízení GDPR je to ideální cesta, jak mít přímo u daného kontaktu – osobního údaje přiložené veškeré důležité dokumenty či souhlasy.

Vůbec prvním krokem je nastavení složky, do které se budou všechny dokumenty ukládat. V agendě Globální nastavení v sekci Dokumenty nejprve zatrhněte možnost Používat složku dokumentů firmy. Poté si všimněte těchto polí:

- **Složka dokumentů** – v tomto poli se automaticky nabídne cesta k adresáři ve vašem počítači. Jde o datovou složku programu POHODA, která se založila automaticky během instalace programu. Doporučujeme toto umístění neměnit.

- **Složka dokumentů firmy** – do tohoto pole POHODA automaticky doplní název vytvářené složky, která bude pojmenována po účetní jednotce, v níž toto nastavení provádíte. Chcete-li složku nazvat jinak, jednoduše do ní klikněte a přepište ji. (Název složky v tomto poli je automaticky zkrácen o doplňky typu s. r. o., a. s. apod.)



Pro vlastní práci se soubory slouží nabídka povelů a tlačítek. V agendě Adresář vyberte záznam, ke kterému chcete přiřadit dokumenty. Nejprve zde klikněte na tlačítko **<<Složka není definována>>**. POHODA zobrazí dialogové okno, ve kterém rovnou nabízí umístění a vytvoření složky pro daný záznam.

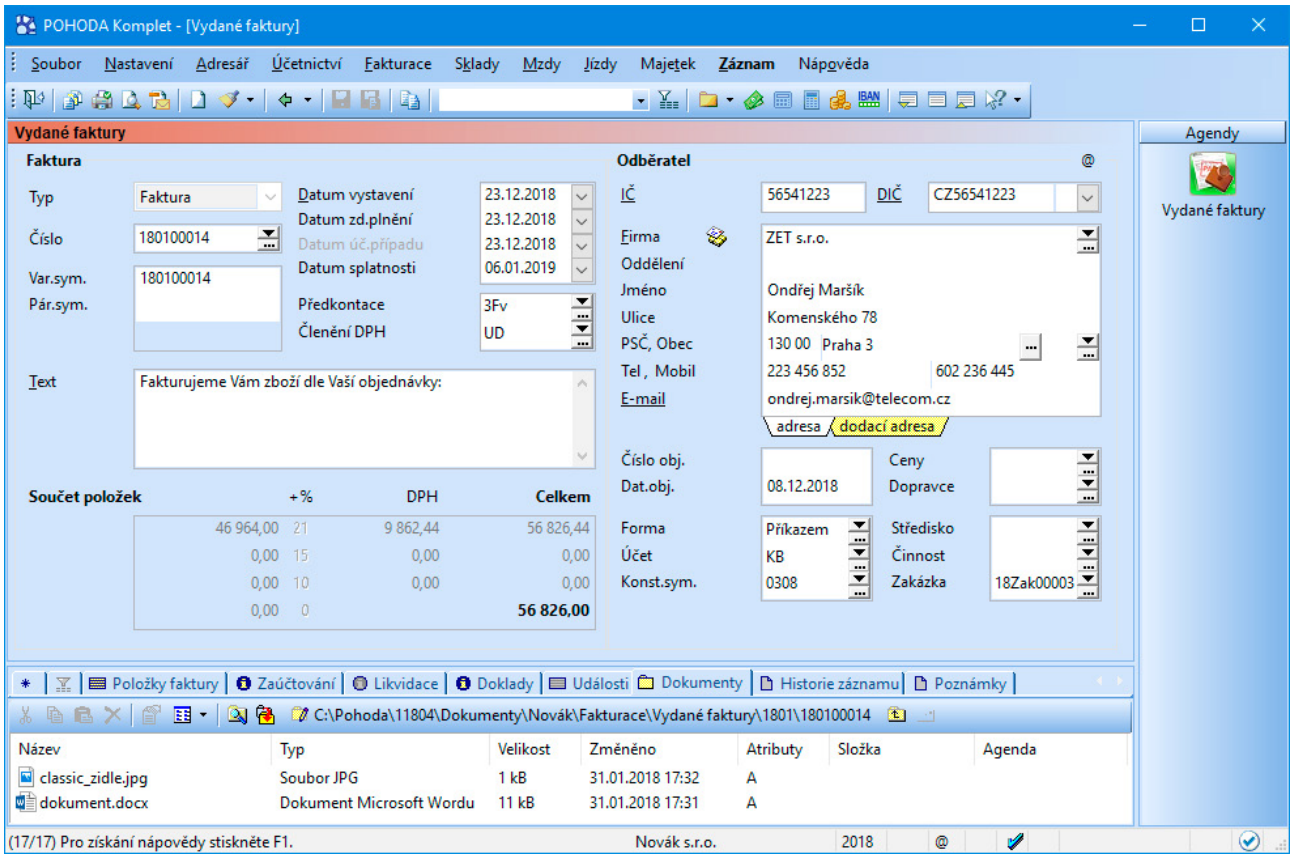
K vybranému záznamu v agendě Adresář vložíte soubor pomocí tlačítka Začlenit soubory. Otevře se okno, ze kterého obvyklým způsobem vyhledáte soubor ze svého počítače. Ve výklopném seznamu můžete vybrat, jakým způsobem se má soubor přenést, a sice:

- **zkopírovat** – vkládaný soubor zůstane na původním místě a jeho kopie se vloží do nadefinované složky pro dokumenty (tato možnost je v dialogovém okně nastavena jako výchozí),

- **vytvořit zástupce** – soubor zůstane stále na původním místě a z programu POHODA se na něj budete pouze odkazovat,

- **přesunout** – soubor se z původního umístění přesune do nadefinované složky.

Jakmile některou z těchto tří operací zvolíte, vybraný soubor se objeví u daného záznamu na záložce Dokumenty programu POHODA.



Pokud na nějaký soubor na záložce Dokumenty kliknete, aktivují se další tlačítka pro práci se souborem:

– tlačítka pro vyjmutí, zkopírování a vložení souboru do složky

– tlačítko pro vymazání souboru ze složky dokumentů

– tlačítko pro nastavení vlastností souboru

– tlačítko, kterým ovlivníte zobrazení souborů ve složce dokumentů

– tlačítko pro otevření složky dokumentů v aplikaci Průzkumník

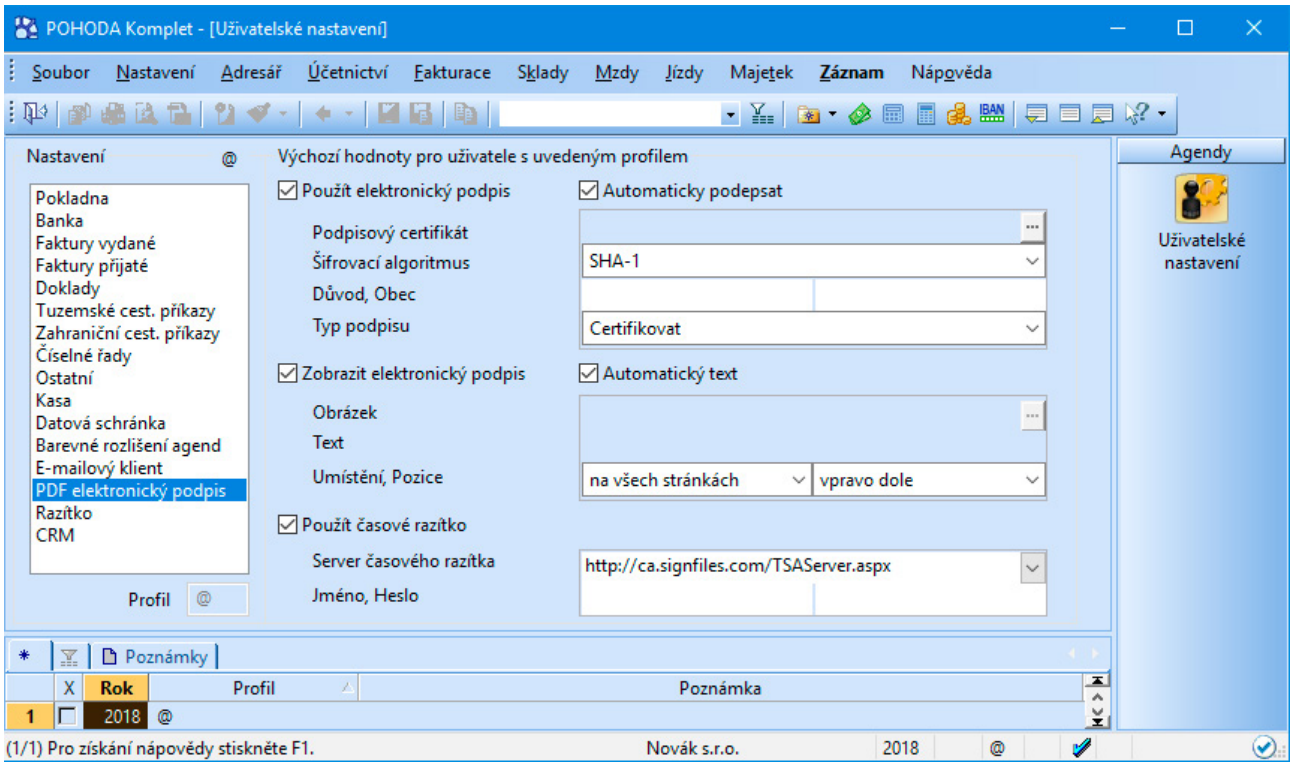
– tlačítko pro vytvoření nebo přejmenování složky

– tlačítko pro odeslání dokumentu e-mailem

5.5. Podepisování PDF dokumentů

Doposud byla řeč především o dokumentech, které do programu POHODA k jednotlivým záznamům přiřazujete z externích úložišť, za účelem přehlednější správy osobních údajů. Teď něco o dokumentech vygenerovaných z programu POHODA. Podle nařízení GDPR totiž musíte vědět, kdo osobní údaje jakkoliv zpracovával – tím se samozřejmě myslí i generování PDF dokumentů, jejichž součástí tyto osobní údaje jsou. Jak tedy poznáte, kdy a kdo vytvořil konkrétní PDF dokument z programu POHODA? Jednoduše, stačí konkrétnímu uživateli nastavit časové razítko a elektronický podpis přímo v agendě Uživatelské nastavení.

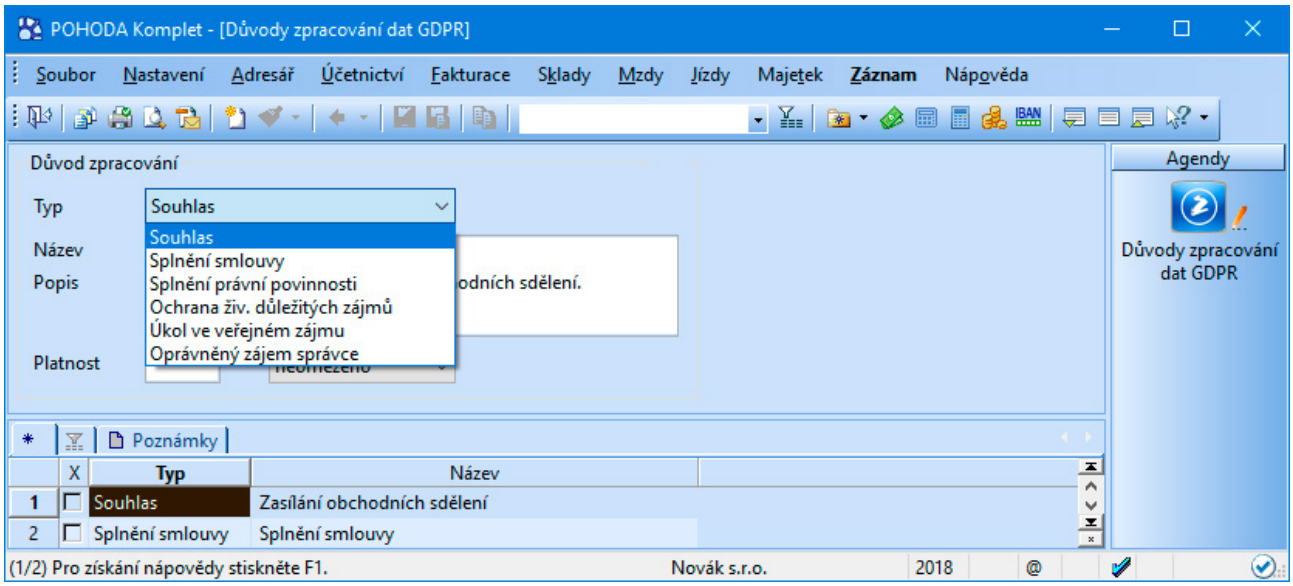
Po zatržení volby **Použít elektronický podpis** v sekci PDF elektronický podpis vyberte šifrovací algoritmus, typ podpisu, podpisový certifikát a zadejte údaje, které se budou zobrazovat ve vlastnostech podpisu vytvořeného PDF dokumentu. Pokud zatrhnete volbu **Zobrazit elektronický podpis**, bude automaticky nastaven výchozí obrázek a text podpisu. Text i obrázek podpisu si můžete zvolit podle svého. Při použití časového razítka si můžete vybrat server pro ověřování časového okamžiku, před kterým dokument zaručeně existoval. Časové razítko obsahuje především aktuální datum a čas, sériové číslo razítka a identifikaci autority, která toto razítko vydává. Pro přístup na server je důležité zadat jméno a heslo uživatele.



Veškeré údaje, které k podepisování PDF dokumentů zadáte v agendě Uživatelské nastavení, můžete dodatečně nebo operativně změnit v dialogovém okně Elektronické podepsání PDF, které se zobrazuje při vytváření PDF dokumentu.

6. Důvody zpracování osobních údajů

POHODA obsahuje speciální agendu, ve které jsou právní důvody zpracování osobních údajů už předdefinované. Agenda vám však poskytuje také maximální prostor pro zapsání důvodů vlastních – přece jen, každý obor podnikání zahrnuje specifické služby, a tím pádem existuje mnoho okolností zpracování údajů. Při zápisu nového záznamu (důvodu) stačí vyplnit předdefinovaná pole formuláře. Tyto záznamy pak můžete přiřazovat k jednotlivým záznamům v agendě Adresář. Agendu Důvody zpracování dat GDRP naleznete v nabídce Nastavení/Seznamy.



Jaké důvody si do agendy programu POHODA zapíšete, je jen na vás. Nezapomínejte však na zákonné důvody, které by měly předcházet těm, pro které potřebujete souhlas subjektu údajů. Platná legislativa například nařizuje podnikatelům, účetním jednotkám a dalším subjektům archivovat po stanovenou dobu účetní doklady, které samozřejmě mnohdy obsahují údaje o zaměstnancích, společnících, obchodních partnerech nebo třeba zákaznících. Podívejte se na malý přehled toho, jaké dokumenty jste povinni uchovávat právě ze zákonného důvodu. Archivačních lhůt a výjimečných situací je však opravdu hodně, proto se vždy musí brát v potaz, o jaký dokument se jedná a jaké pro něj v dané situaci platí lhůty úschovy.

Typ dokumentu	Doba archivace	Dle zákona
Podnikatel, který není dle zákona o účetnictví účetní jednotkou (tj. neplátce DPH, vedoucí daňovou evidenci nebo uplatňující výdaje paušálem)		
dokumenty potřebné k daňové kontrole	3 roky (možnost prodloužení lhůty o 10 let)	č. 280/2009 Sb., daňový řád – § 92 (3), § 93 a § 148
Účetní jednotka (podle zákona o účetnictví)		
účetní závěrky a výroční zprávy	10 let	č. 563/1991 Sb., o účetnictví – § 31 a § 32
účetní doklady, účetní knihy, odpisové plány, inventurní soupisy, účtový rozvrh, přehledy	5 let	
účetní záznamy, kterými účetní jednotky dokládají vedení účetnictví (daňové doklady aj.)	5 let	
Podnikatelé (plátci DPH) i účetní jednotky		
doklady od osob povinných k dani z přidané hodnoty	10 let	č. 235/2004 Sb., o dani z přidané hodnoty – § 35 a § 35a

Zaměstnavatelé		
stejnopisy evidenčních listů	3 roky	č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení – § 35a (4) a § 37 (1)
seznam společníků a členů statutárního orgánu dozorčí rady společnosti za jednotlivé kalendářní měsíce (před rokem 2014, od 1. 1. 2014 je tato povinnost zrušena) a přehled kalendářních měsíců, za které společnost neodvedla pojistné na sociální zabezpečení a příspěvek na státní politiku zaměstnanosti	6 let (3 roky po úhradě pojistného)	
mzdové listy (mzdové listy poživatelů starobního důchodu)	30 let (10 let)	
údaje potřebné pro stanovení a odvod pojistného	10 let	č. 589/1992 Sb., o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti – § 22c
vnitřní předpis, kterým zaměstnavatel stanovuje práva z pracovněprávních vztahů výhodněji	10 let	č. 262/2006 Sb., zákoník práce – § 305 (4)

Obchodní společnosti a družstva (s výjimkou družstev bytových)		
zakladatelské dokumenty, statuty, stanovy, jednací řády, organizační řády a schémata, dokumenty o přeměnách právnických osob, dokumentace o zrušení a zániku	Dle vnitřní směrnice, resp. skartačního plánu, vždy se souhlasem příslušného státního oblastního archivu	č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů – § 3 (2), Příloha č. 1
protokoly a zápisy z jednání statutárního orgánu a dozorčího orgánu, zprávy dozorčího orgánu, zápisy z valných hromad s přílohami, výroční zprávy, zprávy o auditu		
mimořádné inventarizace majetku při vzniku, dělení nebo likvidaci společností, smlouvy o převodu vlastnického práva k nemovitostem a listiny osvědčující přechod vlastnického práva k nemovitostem, dokumentace zápisu a certifikace ochranných známek		
finanční dokumenty (účetní závěrky)		
podnikatelské záměry, vývojové studie, dokumentace výrobků (finální výkresy sestavení či sestav, prospekty, katalogy, vzorkovnice)		

7. Bezpečnost dat v programu POHODA

GDPR se dotýká především otázky ochrany soukromí a pro nás ve STORMWARE je právě bezpečnost dat prioritou č. 1. Stupeň zabezpečení údajů zpracovávaných v ekonomickém systému POHODA závisí především na použité technologii, která se liší v závislosti na řadě programu – POHODA, POHODA SQL a POHODA E1.

7.1. Základní řada POHODA

Základní řada programu POHODA využívá technologii file-server, což znamená, že každý uživatel pracuje s daty, která jsou uložená přímo v jeho počítači (v případě síťové varianty pak na firemním serveru). Samotná data jsou zabezpečena pomocí ověření uživatelského hesla a systému základních přístupových práv. To znamená, že uživatelům můžete přidělit přístupová práva k dílčím agendám a funkcím.

A jak na to? V programu POHODA si z nabídky Nastavení otevřete agendu Přístupová práva/Uživatelé. Přístup má do ní pouze administrátor (nebo uživatel, kterému přiřadil právo k provádění této operace). Na záložce Uživatel vyberte toho, komu chcete práva změnit, a na záložce Práva zvolte ve stromové struktuře konkrétní oblast, například Účetnictví, Mzdy nebo třeba Přijaté faktury. V sekci Práva ve zvolené úrovni pak už můžete uživateli nastavit, jaké operace bude smět se záznamy provádět. Při práci v dané oblasti se mu pak dole na příkazové řádce zobrazí ikonka označující právě jeho oprávnění:

žádná práva – uživatel nemá pro danou položku/agendu žádná práva

čtení – uživatel má právo prohlížet záznamy, ale nemůže je jakkoliv měnit nebo přidávat

zápis – uživatel může prohlížet záznamy a přidávat další

zápis a modifikace vlastních – uživatel má právo prohlížet záznamy, přidávat další, vlastní záznamy může i měnit

zápis a modifikace všech – uživatel může prohlížet, přidávat a měnit všechny záznamy

všechna (včetně mazání) – uživatel smí přidávat, prohlížet, měnit a mazat všechny záznamy

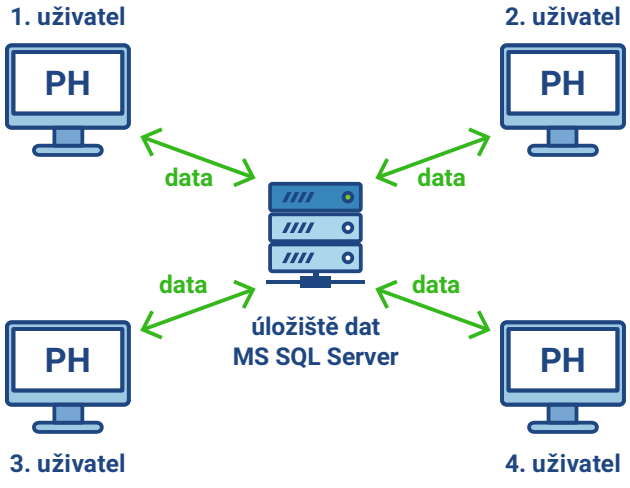
V programu POHODA můžete také sledovat historii změn, ve většině agend tak uvidíte, kdo a kdy záznam vytvořil a uložil, stačí mít v Globálním nastavení v sekci Historie zatrženou volbu Evidovat historii změn. Pokud navíc chcete zobrazit u agendy i záložku Historie změn, zaškrtněte volbu Záložka. Jednotlivé záznamy jde také zamknout, aby nedocházelo k nežádoucím zásahům. Tento způsob zabezpečení je pro menší firmy, které pracují s malým objemem dat, zcela dostačující, program pracuje rychle a je bezpečný.

7.2. Řady POHODA SQL a POHODA E1

tip

Pro větší firmy, které zpracovávají spoustu dat, jsou vhodnější řady POHODA SQL a E1, a to nejen kvůli rychlosti a výkonu, ale i kvůli vyššímu stupni zabezpečení dat. Využívají totiž technologii SQL. To znamená, že vaše data jsou uložena na zabezpečeném Microsoft SQL Serveru, kde je veškerá manipulace s nimi dokumentována. SQL server má navíc k dispozici administrátorské nástroje pro správu systému, dat a sledování provozu databázového stroje.

Jednou z výhod řad POHODA SQL a E1 tedy je, že uživatelé programu nemají přístup přímo ke zdrojovým datům, ta jsou uložena právě na SQL serveru. Po síti se přenáší vždy pouze ty záznamy, které v dané chvíli uživatel přímo potřebuje. Vaše citlivá data jsou tak více chráněna proti poškození a neoprávněnému přístupu nebo jejich zneužití. Zároveň je tento přístup i rychlejší, při práci s velkým množstvím dat nebo souběžné práci více uživatelů nedochází k žádnému zdržování.



Uživatelé mají k dispozici pouze ta data, která zrovna potřebují

V řadách POHODA SQL a E1 navíc dokážete své záznamy vícefázově zamknout či využívat rozšířená přístupová práva, např. na číselné řady či exporty agend. Taky lze určitým uživatelům omezit přístup k záznamům s vybranými číselnými řadami, k osobním údajům vašich zákazníků se tak dostanou pouze ti, kteří to nutně potřebují ke své práci. Například definicí práv pomocí rolí přidělíte přístupová práva jednotlivým pracovním pozicím – jiná budou mít účetní, jiná skladníci.

Pro instalaci řad pracujících s SQL technologií potřebujete Microsoft SQL Server. Konkrétní systémové požadavky na pracovní stanice jednotlivých uživatelů pak najdete na www.stormware.cz/systemove-pozadavky/.

Doporučujeme přejít na řadu POHODA SQL nebo E1, pokud…

…požadujete vysokou úroveň zabezpečení dat.

…potřebujete ke svým datům přistupovat vzdáleně.

…chcete sami vytvářet uživatelské agendy bez použití externí aplikace.

…velikost vaší největší databáze (účetní jednotky) dosahuje 70 MB a více.

…vzhledem ke svým podnikatelským aktivitám plánujete nárůst objemu dat.

…využíváte velké množství účetních jednotek.

Co to znamená SQL?

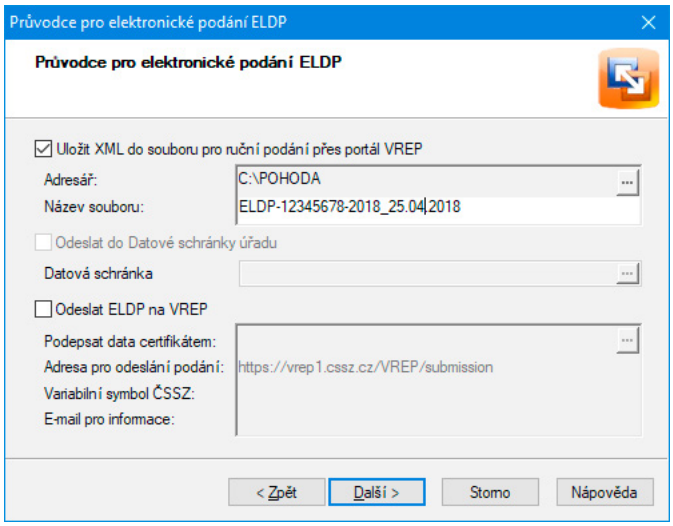
Pod zkratkou SQL se skrývá pojem Structured Query Language, což bychom mohli přeložit jako strukturovaný dotazovací jazyk. Jde o jednoduchý a zároveň robustní nástroj pro jednotnou úroveň přístupu k datům v datových úložištích. SQL jazyk není závislý na dalších vývojových a implementačních nástrojích, neobsahuje totiž samostatné nástroje pro tvorbu aplikací.

V souladu s bezpečnostním ustanovením GDPR doporučujeme vést databázi fyzických osob – zákazníků odděleně od databáze fyzických osob – zaměstnanců. A to především v případě, že jsou tyto databáze většího rozsahu (tj. zaměstnáváte větší počet zaměstnanců). Pro jejich oddělenou správu tak doporučujeme vedle ekonomického systému POHODA využít **personální a mzdový systém PAMICA**, který obstará celou personální agendu.

7.3. Přenos dat z/do programu POHODA

Když máte vyřešené zabezpečení dat v programu POHODA a nastavený propracovaný systém přístupových práv, nezapomeňte také na přenos údajů z/do programu POHODA. Data ze svého ekonomického systému zajisté odesíláte třetí straně (ať už jsou to faktury zasílané zákazníkům, nebo přehledy na příslušnou správu sociálního zabezpečení) nebo je naopak od třetí strany přijímáte a do programu následně importujete (např. když máte s programem POHODA propojený e-shop nebo jinou externí aplikaci). Mnohdy jde o ty nejcitlivější informace – proto čím méně „prostředníků", tím lépe.

Oficiální dokumenty snadno odešlete do datové schránky úřadů nebo do aplikace finanční správy a ČSSZ přímo z programu POHODA. Pomůže vám s tím průvodce pro elektronické podání, kterého vyvoláte prostřednictvím povelu pod nabídkou Záznam u daného přiznání, resp. přehledu. Takto odeslaná data jsou vždy zašifrována a opatřena elektronickým podpisem.



Při běžném odesílání tiskových výstupů (třeba vydaných nabídek e-mailem) je alespoň zaheslujte – stačí upravit nastavení tisku (ve výklopném menu PDF/Nastavení PDF… zadejte na záložku Zabezpečení požadované heslo tiskové sestavy).

TIP *Využíváte služeb technické podpory STORMWARE? Pak pro bezpečný přenos databází používejte servisní schránku dostupnou na www.stormware.cz/schranka.*

8. GDPR v praxi

Implementace nařízení GDPR do praxe je pro mnohé podnikatele nepředstavitelná. Vybrali jsme pro vás pár příkladů ze života, díky kterým si lépe představíte zpracování osobních údajů ve spolupráci s programem POHODA.

Marketingová agentura

Jako marketingová agentura máte na svých webových stránkách možnost jednorázové registrace k odběru newsletteru – e-booku s marketingovými tipy. Registrace má omezenou platnost 3 měsíce, po tuto dobu uživatelům každý týden chodí část e-booku. V programu POHODA si tak nadefinujete nový důvod zpracování osobních údajů, „Zasílání reklamních sdělení", na základě poskytnutého souhlasu s platností 3 měsíce. Tento důvod přiřadíte konkrétním adresám na záložce GDPR.

Před koncem souhlasu (například po 2 měsících od registrace) si tyto adresy můžete jednoduše vyfiltrovat a zaslat jim vlastní nabídku profesionální marketingové komunikace. Poté, co se ji 100 uživatelů (z původních 350 registrovaných) rozhodne využít, přiřadíte jim další důvod zpracování údajů, tentokrát na základě smluvního vztahu. Mezitím si jeden z těchto uživatelů vyžádá doložit data, jaká o něm zpracováváte. Na pár kliknutí si tak zobrazíte, jaká data o něm evidujete a na základě čeho – v tomto případě rovnou ze dvou důvodů: zasílání reklamních sdělení a smluvního vztahu.

OSVČ – technik

Prodáváte, montujete a opravujete plynové kotle, tyto služby propagujete také na svých webových stránkách. Pan Novák se přihlásil k odběru obchodních sdělení, která obsahují praktické informace o revizi kotle. Do agendy Adresář programu POHODA tak zadáte údaje zadané při registraci (jméno a e-mail) a na záložku GDPR také informace o jejich zpracování na základě souhlasu se zasíláním obchodních sdělení.

Poté vás pan Novák telefonicky kontaktuje a chce zpracovat nezávaznou nabídku. Pro tyto účely vám poskytne znovu své jméno a e-mail, ale také adresu s telefonem. Doplníte tedy chybějící údaje k jeho záznamu do adresáře a v agendě Vydané nabídky vystavíte požadovanou nabídku na plynový kotel. Informace o vystavené nabídce se propíše také do agendy Adresář na záložku GDPR, a to jako vystavený předprodejní doklad. Stačí zvolit povel Aktualizovat data použití adresy… z nabídky Záznam.

- Pokud nabídku pan Novák nakonec nevyužije, měli byste po vámi stanovené době jeho adresu a telefon v souladu s GDPR z adresáře vymazat. (Jméno a e-mail pana Nováka můžete tak či onak evidovat s neomezenou platností, dokud souhlas se zasíláním obchodních sdělení neodvolá.)

- Jestli si kotel nakonec koupí, vystavíte mu v agendě Vydané faktury prodejní doklad. Tato informace se pak objeví také v adresáři na záložce GDPR ve formě data vystavení prodejního dokladu.

Účetní

Jako účetní zpracováváte daňovou evidenci, popř. účetnictví 25 podnikatelům a firmám. Protože účetní data obsahují také nespočet osobních údajů, jste zákonitě jejich zpracovatel a vaši klienti jsou jejich správci. Kromě jejich evidence v účetním programu máte potřebnou dokumentaci (faktury, dodací listy apod.) zařazenou v šanonech. Jak postupovat?

V prvé řadě si ošetřete zpracování údajů a jejich zabezpečení smluvně se všemi 25 klienty, kde bude mimo jiné upraveno ukládání dat v účetním programu i zmíněných šanonech. Důležitá bude také bezpečnost přenosu dat klient-účetní. Veškeré výstupy z účetního programu pro jistotu opatřete heslem – POHODA to umožňuje nastavit přímo během exportu dokumentu v dialogovém okně Tisk.

Na závěr je důležité říct, že veškerá iniciativa by měla vycházet od vašich klientů, jelikož oni jsou správci údajů.

E-shop

Ve svém e-shopu prodáváte ručně vyrobené zboží pro maminky s dětmi. Jelikož údaje svých zákazníků evidujete pro účely plnění smlouvy, tj. na základě objednávky jim zasíláte zboží, není nutné obstarávat souhlas se zpracováním osobních údajů. V programu POHODA tak jednoduše vystavíte fakturu a přímo k údajům zákazníka v adresáři přiřadíte na záložku GDPR účel „Splnění smlouvy" a zadáte dobu její platnosti – po tuto dobu můžete evidovat zákazníkovy osobní údaje. Druhou možností je využít data předprodejních, prodejních a poprodejních dokladů, které POHODA vypisuje na záložku GDPR po vystavení příslušného dokladu a zvolení povelu Aktualizovat data použití adresy… z nabídky Záznam. Samostatný důvod zpracování tak už není potřeba na záložku psát. Jakou cestou se vydáte, je jen na vás – z hlediska GDPR je důležité, aby důvod pro zpracování údajů existoval.

Obstarávání souhlasu vás čeká pouze v případě, že spravujete osobní údaje z jiného než zákonného důvodu – třeba zasíláte slevy a nabídky uživatelům registrovaným k odběru vašich e-mailů. Tyto souhlasy je proto potřeba zrevidovat a upravit podle nařízení GDPR. V programu POHODA pak vybraným kontaktům jednoduše přiřadíte důvod – Souhlas („Zasílání obchodních sdělení").

9. Nejčastější otázky a odpovědi

Plánuje POHODA rozšířit své funkce s ohledem na nařízení GDPR?

Ano, zaměřujeme se zejména na snazší správu osobních údajů, jejich vkládaní, třídění a následné zpracování. Primárně se tato rozšíření budou týkat agendy Adresář. O novinkách v oblasti ochrany osobních údajů v programu POHODA zákazníky budeme průběžně informovat standardními komunikačními kanály (e-mailové zpravodaje, časopis Moje POHODA, internetové stránky aj.).

Co musím připravit, aby bylo vše podle nařízení GDPR splněno? Jak je ekonomický systém POHODA připravený na nařízení GDPR?

Uvedení organizace do souladu s GDPR by mělo primárně vycházet z analýzy práce s osobními údaji, se kterými pracujete, tj. jejich kategorizace a typizace, legitimita jejich získání, minimalizace jejich vlastnictví z hlediska účelu a doby držení, jejich zabezpečení apod. Následně by mělo dojít k přijetí vnitřní koncepce, provedení procesních změn a zavedení opatření, která odpovídají zásadám ochrany osobních údajů tak, jak nařízení vyžaduje. Problematiku vcelku srozumitelně popisuje web https://www.gdpr.cz/gdpr/. K těmto činnostem vám může být software nápomocný, nicméně dokáže pokrýt pouze část požadavků GDPR.

Naše produkty, zejména ekonomický systém POHODA a personální a mzdový systém PAMICA, mají již nyní integrované některé funkcionality směřující k naplnění mnoha dílčích požadavků nařízení GDPR, na dalších rozšířeních pracujeme. Zaměřujeme se zejména na snazší správu osobních údajů, jejich vkládaní, třídění a následné zpracování. Primárně se tato rozšíření budou týkat agendy Adresář. O novinkách v oblasti ochrany osobních údajů v našich programech zákazníky průběžně informujeme, viz např. novinky v produktu POHODA a článek na straně 18 časopisu Moje POHODA Leden 2018 nebo článek na straně 14 časopisu Moje POHODA Říjen 2017. (Informace uvedené v obou vydáních se vztahují vždy k aktuálním verzím programu.)

Budeme si muset koupit novou verzi programu POHODA s kompletní podporou GDPR, nebo potřebné aktualizace poskytnete zdarma?

Uživatelé aktuálních verzí programu POHODA budou mít funkcionality související s plněním Obecného nařízení jako součást aktualizací. Speciálně byste si tak nic nepřipláceli.

Samozřejmě záleží také na vámi použité řadě produktu (https://www.stormware.cz/pohoda/rady/), protože např. POHODA E1 již nyní umožňuje evidovat historii uživatelských úprav v agendě Adresář, vytváření volitelných parametrů apod. Případné nové funkce související s GDPR, které se budou týkat právě možností, které nabízí až řada POHODA E1, nebudou tedy z principu dostupné uživatelům nižších řad programu POHODA.

Poskytnete mi jako zákazníkovi společnosti STORMWARE nějaký dokument, že je ekonomický systém POHODA v souladu s GDPR?

V souvislosti s přijetím GDPR byl do právního řádu z hlediska ochrany osobních údajů zaveden nový institut, a to vydávání osvědčení o ochraně osobních údajů (certifikát), který se uplatní v případě operací zpracování prováděných správcem nebo zpracovatelem a který má osvědčit soulad s nařízením. Vydání osvědčení (certifikátu) má subjektům údajů zajistit, aby rychle mohly u příslušných produktů a služeb posoudit úroveň ochrany osobních údajů. Z toho plyne, že by se vydávání osvědčení (certifikátů) mělo týkat i produktů (software a hardware) a služeb.

V nařízení jsou definovány tři možnosti, jak vybrat subjekt pro vydávání osvědčení (certifikační orgán), jedná se jednak o postup, kdy za stanovených podmínek akredituje subjekty pro vydávání osvědčení (certifikační orgány) přímo příslušný dozorový úřad (v případě České republiky je to Úřad pro ochranu osobních údajů) nebo subjekty pro vydávání osvědčení (certifikační orgány) akredituje vnitrostátní akreditační orgán, kterým je Český institut pro akreditaci. Úřad pro ochranu osobních údajů vybral jako nejvhodnější variantu akreditaci subjektů pro vydávání osvědčení (certifikačních orgánů) prováděné Českým institutem pro akreditaci, o. p. s. (ČIA).

V současné době ještě ČIA neuděluje shora zmíněné certifikáty, a to z důvodu přípravy procesu certifikace. Jakmile bude možné si o certifikaci zažádat, pravděpodobně tak učiníme, co nejdříve to bude možné, abychom mohli doložit soulad požadavků, které GDPR klade na naše programy.

V současné době také připravujeme řadu materiálů mapujících zpracování osobních údajů v rámci našich firemních procesů. Ty, které budou určeny subjektům údajů, budeme postupně zveřejňovat. Budete si tak moci udělat do doby udělení certifikace obrázek, že ochranu osobních údajů bereme vážně a stejně tak i přistupujeme k zapracování úprav, které vyplývají z GDPR v našich programech.

Momentálně tedy není možné doložit oficiální certifikaci souladu s GDPR s jakýmkoliv programem.*

* Aktuální k 15. 2. 2018

Naše firma má zakoupenou licenci programu POHODA od společnosti STORMWARE. Kdo je z pohledu GDPR zpracovatel a kdo správce osobních údajů?

STORMWARE bude vystupovat jako zpracovatel pouze v případech, kdy nám pošlete zákaznická data (vaše nebo vašich zákazníků), resp. kdy bude možné s vašimi daty nebo daty vašich zákazníků pracovat (např. při vzdálené správě, školeních s použitím těchto dat apod.). V takovém případě jste správce osobních údajů a se společností

STORMWARE bude nutné uzavřít zpracovatelskou smlouvu, která bude zpřístupněna nejdéle do doby účinnosti Nařízení 2016/679.

V roli správce bude STORMWARE vystupovat také v ostatních případech, konkrétně v souvislosti s e-mailovými dotazy, zákaznickou podporou a v rámci obchodního vztahu.

V naší firmě pracujeme s účetním systémem POHODA. Kde najdu zpracovatelskou smlouvu?

Zpracovatelskou smlouvu zpřístupníme do doby účinnosti Nařízení 2016/679, naše zákazníky o tom budeme informovat standardními komunikačními kanály.

Platí nařízení GDPR i na kontakty od dodavatelů (fyzických osob), které máme v programu POHODA?

Ano, GDPR se týká i vašich dodavatelů – v případě, že pracujete s osobními údaji fyzických osob těchto firem (zaměstnanců, jednatelů apod.). Pro správu takovýchto údajů doporučujeme využít agendu Adresář a vše potřebné evidovat na záložce GDPR.

Provozujeme e-shop. Objednávky od zákazníků se do programu POHODA přenáší včetně osobních údajů, které zákazníci uvedou v objednávce. Jejich osobní údaje jsou pak automaticky přenášeny a uvedeny na všech dokladech – prodejky, faktury, opravné daňové doklady. Objednávky účtujeme buď:

- **Prostřednictvím agendy Prodejky, pak je prodejka odesílána prostřednictvím EET.**
- **Prostřednictvím agendy Vydané faktury, pak je faktura předávána v rámci kontrolního hlášení.**

Jak máme v tomto případě řešit nařízení GDPR?

Předávání osobních dat mimo vaši společnost na základě zákonných důvodů není v rozporu s Nařízením EU 2016/679. Je třeba vzít v potaz, že toto nařízení se týká pouze zpracování osobních údajů fyzických osob (nikoliv korporací) a obsah datových vět, které v rámci EET a kontrolního hlášení odesíláte servery Finanční správy, obsahují osobní údaje pouze v případě, že je uvedeno DIČ poplatníka (fyzické osoby), jehož součástí je rodné číslo. Avšak i na to již zareagovala legislativa – ústavní soud zrušil od 1. března 2018 některé části zákona o EET, mj. právě povinnost uvádět DIČ na účtenkách.

Soulad vašeho postupu s nařízením GDPR dále potvrzuje i to, že se jedná o vaši zákonnou povinnost – osobní údaje (pokud by v kontrolním hlášení a EET byly obsaženy) předáváte na základě zvláštních zákonů státním institucím. Stejné platí i u jiných případů, ve kterých figurují údaje fyzických osob, například zaměstnanecká data předávaná České správě sociálního zabezpečení, zdravotní pojišťovně, Policii ČR apod.

Co bude nabízet personální a mzdový systém PAMICA v oblasti GDPR?

Od účinnosti GDPR bude software PAMICA zpracovávat veškerá osobní data v souladu s principy tohoto nařízení. Veškeré požadavky, které GDPR na správce klade, tak budou naplněny. Je ovšem nutné brát v potaz skutečnost, že software PAMICA je jen nástroj, který zpracování dat umožňuje, přičemž GDPR je především o procesech a nastavení nakládání s osobními údaji v rámci vaší firmy. Ani sebelepší software za vás proto nevyřeší veškeré povinnosti, které GDPR ukládá.

Jak bude program POHODA zabezpečovat šifrování údajů databáze?

Dle čl. 32 odst. 1 písm. b) nařízení GDPR by mělo být dostačující definování rolí, resp. přístupových práv v programu POHODA (např. k jednotlivým agendám programu). Uživatelé také mohou využít další funkce programu:

1. částečné zabezpečení databáze – tj. databáze budou zabezpečené interním heslem programu a budou tak chráněné proti přístupu jiných programů.

2. úplné zabezpečení – tj. zvolené databáze budou zabezpečené interním heslem programu a svázané se systémovou databází. Heslem, které si sami zvolíte, je chráněný neoprávněný převod databází do jiné instalace programu POHODA. Bez hesla tak není vůbec možné databázi převést do jiné instalace programu.

Jako další stupeň ochrany údajů je případně možný přechod na vyšší řadu programu – POHODA SQL nebo POHODA E1 – kde použitá technologie klient-server a databáze SQL poskytuje ještě vyšší stupeň ochrany dat.

S ohledem na samotné nařízení GDPR a na výše uvedené důvody se data v databázích ekonomického systému POHODA nešifrují. Pro úplnost uvádíme i citaci příslušné části nařízení GDPR:

Článek 32 – Zabezpečení zpracování

1. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná **technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně**:

- pseudonymizace a šifrování osobních údajů;
- **schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování**;
- schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
- procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Na školení GDPR mi řekli, že je potřeba vést účetní databázi od té zaměstnanecké odděleně. Je to pravda?

V souladu s bezpečnostním ustanovením GDPR doporučujeme stejně jako váš školitel vést databázi fyzických osob – zákazníků odděleně od databáze fyzických osob – zaměstnanců. A to především v případě, že jsou tyto databáze většího rozsahu (tj. zaměstnáváte větší počet zaměstnanců). Pro jejich oddělenou správu tak doporučujeme vedle ekonomického systému POHODA využít personální a mzdový systém PAMICA, který obstará celou personální agendu.

Jakým způsobem je nejvhodnější získat souhlas ve vztahu k osobním údajům dle zákona č. 101/2001 Sb.? Stačí e-mailem?

Souhlas je nutné především prokázat. Musí být tedy zaznamenán prokazatelně a musí být v případě potřeby doložitelný, v tomto ohledu není problém ho mít e-mailem. Dále souhlas musí být dobrovolný, nelze jím podmínit čerpání nějaké služby. Musí být také jednoznačný v účelu a rozsahu, musí být oddělený například od obchodních podmínek, nesmí být schovaný ve smlouvách apod. Také musí být stanoveno, za jakým účelem je poskytnut, například za účelem zasílání obchodních sdělení. A v neposlední řadě musí být souhlas informovaný, tj. musí být jasné, komu je souhlas udělen, že se nepředává mimo EU a jak je možné jej odvolat.

Bude vhodné souhlas se zpracováním osobních údajů promítnout v obchodních podmínkách?

U souhlasu je důležitý jednoznačný projev vůle subjektu údajů (souhlas tedy musí být udělen jednoznačným projevem vůle osoby). Z tohoto projevu musí být zjevné, že osoba skutečně chtěla udělit souhlas se zpracováním osobních údajů, nikoliv, že pouze vyjadřovala souhlas s obchodními podmínkami uzavřením smlouvy, popř. že pouze nevyjádřila nesouhlas. Proto by takovýto souhlas neměl být součástí všeobecných obchodních podmínek, měl by být naopak oddělený.

Osobní údaj je dle GDPR i evidence o docházce zaměstnance. V práci na chodbě máme docházkové hodiny a vedle nich jsou v kastlíku karty zaměstnanců s evidencí docházky v aktuálním měsíci, jak to lze ošetřit vzhledem ke GDPR?

Osobními údaji jsou veškeré informace o fyzické osobě (subjektu údajů), kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor. Je to například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Z tohoto pohledu karty zaměstnanců obsahují osobní údaje a Nařízení 2016/679 se na jejich zpracování vztahuje, i když se jedná o fyzické záznamy. Důvodem evidence docházky je na vaší straně splnění právní povinnosti a opět je na vás, jakým způsobem zajistíte ochranu těchto osobních v souladu s čl. 32 Nařízení. Je potřeba nastavit přiměřená technická i organizační opatření.

Jak doporučujete řešit marketingové e-maily, co se týče GDPR?

Zde je situace trochu složitější, protože marketingové e-maily můžeme rozdělit do dvou skupin:

- E-mailing, který se jako marketingový může tvářit, ale obsahuje informace například o skutečnosti, že objednaná služba již končí, a vy příjemce informujete o službě nové či lepší. To může být chápáno jako oprávněný zájem správce, kdy uplatníte legitimní titul – smluvní vztah a nepotřebujete tedy žádný další souhlas subjektu.

- E-mailingová sdělení, typicky obsahující nějaký produkt či službu nesouvisející s již poskytovanou službou či dodaným produktem, postrádá oprávněný zájem správce. Proto je potřeba na takovýto e-mailing mít již předem souhlas subjektu se zasíláním obchodních sdělení.