

Nariadenie GDPR a program POHODA

STORMWARE
POHODA
Ekonomický systém

www.pohoda.sk

Obsah

1.	Úvod	3
2.	O európskom nariadení GDPR	4
2.1.	Čo je teda GDPR?	4
2.2.	Kedy bude GDPR platiť?	4
3.	Základné GDPR pojmy	5
4.	Ako sa pripraviť na GDPR	6
4.1.	Interný audit	6
4.2.	Interný systém	7
4.3.	IT systém	7
4.4.	Zoznam nových povinností	8
4.5.	Analýza rizík	9
4.6.	Opatrenia na odstránenie rizík	10
5.	Správa osobných údajov v programe POHODA	11
5.1.	Vyhľadanie, úprava a vymazanie osobných údajov	12
5.2.	História záznamov	16
5.3.	Súpiska s údajmi vybranej dotknutej osoby	16
5.4.	Práca s dokumentami	17
5.5.	Podpisovanie PDF dokumentov	18
6.	Dôvody spracúvania osobných údajov	20
7.	Bezpečnosť dát v programe POHODA	22
7.1.	Základný produktový rad POHODA	22
7.2.	POHODA SQL a POHODA E1	22
7.3.	Prenos dát z/do programu POHODA	23
8.	GDPR v praxi	24
9.	Najčastejšie otázky a odpovede	25

1. Úvod

Asi každý podnikateľ nejakým spôsobom nakladá s osobnými údajmi svojich zákazníkov, obchodných partnerov alebo zamestnancov. Aj preto sa európske nariadenie dotýka toľkých jednotlivcov a firiem. Ekonomický systém POHODA sa na GDPR samozrejme pripravuje, pre užívateľov bude plniť funkciu nástroja, ktorý spracovávanie osobných údajov čo najviac uľahčí.

V našom návode si priblížime, čo je podstatou nariadenia GDPR, ako sa naň pripraviť a predovšetkým na čo nezabudnúť. V jeho druhej časti sa potom dozvieme o správe údajov v ekonomickom systéme POHODA v súlade s GDPR, o možnostiach zabezpečenia údajov a tiež o niektorých príkladoch z praxe, vďaka ktorým možno lepšie pochopíte základné princípy tohto európskeho nariadenia. Na záver vás čaká výber otázok od užívateľov programu POHODA na tému GDPR a našich odpovedí na ne – týkajú sa samotného programu i správy osobných údajov všeobecne.

2. O európskom nariadení GDPR

Nariadenie GDPR (General Data Protection Regulation) výrazným spôsobom prepracováva legislatívu na ochranu osobných údajov. Reaguje na súčasnú dobu, v ktorej sa informačné systémy a digitálne podnikanie všeobecne stávajú neoddeliteľnou súčasťou takmer každej firmy. Dobu, v ktorej celý rad firiem využíva na komerčné účely pojem big data alebo, lepšie povedané, zbiera informácie, ktoré po sebe v kyberpriestore zanechávame.

Nariadenie je jedným z najrozsiahlejších právnych predpisov, ktoré Európska únia v posledných rokoch prijala. Dokonca i skutočnosť, že sa nejedná o smernicu, ale priamo o nariadenie, robí z GDPR mimoriadny právny predpis, ktorý špecialisti na ochranu údajov analyzujú a formou sprievodných pokynov dotvárajú. Bez zveličovania možno povedať, že sa jedná o najväčšiu zmenu legislatívy v oblasti nakladania s osobnými údajmi za posledných 20 rokov.

GDPR sa týka plošne všetkých firiem, ktoré spravujú, zhromažďujú či spracúvajú osobné údaje občanov Európskej únie. V našom podnikateľskom prostredí sa tak bude jednať o všetky firmy a jednotlivcov, ktorí spracúvajú osobné údaje svojich zamestnancov, zákazníkov alebo dodávateľov. GDPR sa ale uplatní i na tých, ktorí sledujú a analyzujú chovanie užívateľov na webe prostredníctvom nástrojov ako je Google Analytics alebo Facebook. Cieľom GDPR je totiž chrániť digitálne práva občanov EÚ.

2.1. Čo je teda GDPR?

Nariadenie GDPR nanovo reguluje spracovávanie osobných údajov fyzických osôb, konkrétne upravuje tie oblasti, kde sa dnes riadime zákonom 122/2013 Z.z. o ochrane osobných údajov. GDPR zavádza celý rad nových práv a povinností a tiež spresňuje či sprísňuje existujúce pravidlá.

2.2. Kedy bude GDPR platiť?

Nariadenie GDPR predstavuje záväznú normu, ktorá vstúpila do platnosti v máji 2016 a musí byť zavedená od 25. mája 2018 v celom svojom rozsahu vo všetkých štátoch EÚ.

3. Základné GDPR pojmy

Na začiatku je najdôležitejšie porozumieť základným GDPR pojmom – potom vám bude hneď jasnejšie, či sa vás GDPR vôbec týka.

Čo všetko je osobný údaj?

Osobný údaj je akákoľvek informácia o konkrétnej fyzickej osobe. Keď sa povie Ján Nový, ešte to nie je možné chápať ako osobný údaj – Nových je viacero. Ak sa ale táto informácia spojí s ďalším údajom, ktorý už by identifikoval Jána Nového ako konkrétnu osobu (napríklad adresa Palackého 1, Bratislava), potom už sa jedná o osobný údaj. Okrem adresy, čísla a iných identifikátorov to môže byť i akákoľvek fyzická, fyziologická, genetická, psychická, ekonomická, kultúrna alebo spoločenská črta tejto fyzickej osoby.

Čo sú citlivé osobné údaje?

Spracúvanie citlivých osobných údajov podlieha oveľa prísnejšiemu režimu ako všeobecné údaje, pretože môžu subjekty týchto údajov poškodiť v spoločnosti, v zamestnaní, v škole, či môžu zapríčiniť ich diskrimináciu. Jedná sa o údaje o rasovom či etnickom pôvode, politických názoroch, náboženskom alebo filozofickom vyznaní, členstve v odboroch, o zdravotnom stave, sexuálnej orientácii a trestných deliktach či o právoplatnom odsúdení osôb.

Čo sa myslí spracúvaním osobných údajov?

Spracúvanie osobných údajov je akákoľvek operácia, kedy sa s údajmi nejako manipuluje. Môže to byť napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, prenos, ale i vymazávanie či likvidácia údajov, pričom nezáleží na tom, či je to strojovo alebo ručne. Spracúvanie skrátka obsahuje všetky činnosti, pri ktorých je osobný údaj „prítomný“.

Kto je dotknutá osoba?

Dotknutou osobou je žijúca fyzická osoba, ktorej sa osobné údaje týkajú.

Kto je prevádzkovateľom osobných údajov?

Prevádzkovateľom je subjekt akejkoľvek právnej formy, ktorý za spracúvanie primárne zodpovedá. Určuje účely a prostriedky spracúvania osobných údajov.

Kto je sprostredkovateľom osobných údajov?

Sprostredkovateľ osobných údajov spracúva osobné údaje v mene prevádzkovateľa. Vždy ale vykonáva len také operácie, ktorými ho prevádzkovateľ poverí alebo aké vyplývajú z jeho doterajšej činnosti. Môže sa jednať napríklad o externú účtovníčku, ktorá pre podnikateľa spracováva osobné údaje klientov.

Kto je zodpovedná osoba pre ochranu osobných údajov?

Zodpovedná osoba pre ochranu osobných údajov (Data Protection Officer alebo skrátene DPO) môže byť zamestnancom vašej firmy alebo môže úlohy plniť na základe zmluvy o poskytovaní služieb. Zároveň to môže byť právnická i fyzická osoba.

DPO v rámci vašej firmy poskytuje poradenstvo a informácie o povinnostiach podľa GDPR, spolupracuje s dozorným orgánom a pôsobí ako kontaktné miesto pre dozorný orgán. Nariadenie GDPR priamo definuje, kto takúto zodpovednú osobu potrebuje:

- úrad (štátna správa) či verejný subjekt,
- firma, ktorej hlavná činnosť spočíva v spracovateľských operáciách, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu,
- firma, ktorej hlavná činnosť spočíva v rozsiahlom spracúvaní zvláštnych kategórií údajov alebo spracúvaní osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky.

4. Ako sa pripraviť na GDPR

Príprava na GDPR môže zabráť i niekoľko mesiacov, a preto ju rozhodne nenechávajte na poslednú chvíľu. Ak ste navyše väčšia firma, oplatí sa dohodnúť si odbornú pomoc. Predsa len ide o rozsiahle nariadenie, s ktorým sa i odborníci iba nedávno zoznámili, a tak pravdepodobne nebude vo vašich silách všetko zvládnuť svojpomocne.

Táto kapitola vám pomôže zorientovať sa v danej oblasti – prehľadne totiž uvidíte, čo všetko musíte prejsť, zanalyzovať, či upraviť.

4.1. Interný audit

Hneď na začiatku si zosumarizujte, aké osobné údaje spracúvate, kto a ako s nimi nakladá a ako sú zabezpečené, tiež aj to ako ich archivujete, prenášate alebo likvidujete. Jednoducho zhodnoťte aktuálny stav ochrany osobných údajov vo vašej firme a všetky nedostatky voči novým povinnostiam, ktoré vám GDPR ukladá. V tomto kroku si musíte odpovedať napríklad na tieto otázky:

- 1. Aké spracúvanie vykonávam, najmä v personálnej a klientskej agende?**
 - Sú osobné údaje spracúvané manuálne alebo automatizovane?
- 2. Prečo a na základe akého právneho titulu osobné údaje spracúvam?**
 - Na plnenie úloh ukladaných zákonom? Napr. vedenie agendy pre účely sociálneho poistenia.
 - Pre iné účely? Najmä plnenie zmluvy, plnenie podnikateľského zámeru na základe súhlasu dotknutej osoby, s využitím verejných zdrojov, na ochranu práv prevádzkovateľa a pod.?
 - Splňam požiadavky pre zákonné spracúvanie?
 - Udal som dostatočný dôvod pre spracúvanie osobných údajov?
- 3. V akom rozsahu sa osobné údaje zhromažďujú?**
 - Vykonávam spracúvanie údajov podľa účelu, ktorý som špecifikoval?
 - Sú zhromaždené údaje adekvátne, presné a účelné?
- 4. V akom termíne sa osobné údaje likvidujú?**
 - Uchovávam osobné údaje iba na čas nevyhnutne potrebný?
- 5. Akým spôsobom sa osobné údaje aktualizujú?**
 - Sú zhromaždené údaje presné a aktualizované podľa potreby?
- 6. Komu môžu byť osobné údaje sprístupnené vo firme alebo v rámci mojich podnikateľských aktivít?**
- 7. Mám stanovené interné normy týkajúce sa spracúvania osobných údajov?**
- 8. Kto je za dodržiavanie internej normy týkajúcej sa vyššie uvedených bodov zodpovedný?**
- 9. Kto je zodpovedný za komunikáciu s dotknutými osobami?**
 - Mám k dispozícii procedúru na určenie práv dotknutých osôb s ohľadom na ich údaje, ktoré spracúvam?
- 10. Chránim dostatočne osobné údaje?**
 - Zabraňujú používané technické prostriedky a uplatňované organizačné opatrenia náhodnému prístupu k osobným údajom, ich zmene, zničeniu alebo strate?
- 11. Mám k týmto bodom vôbec nejakú dokumentáciu?**
(Ak nie, založte si ju a udržiavajte aktuálnu.)

4.2. Interný systém

Najlepšie v spolupráci s právnikom nastavte vo vašej firme také opatrenia, ktoré budú zodpovedať nárokom GDPR. Vychádzajte pritom z vykonaného interného auditu a zamerajte sa okrem iného na nasledujúce oblasti:

1. **Detailný prehľad spracúvania osobných údajov** vo vašej organizácii podľa jednotlivých agend (napr. personálna, dodávateľská, odberateľská), ktorý bude obsahovať nasledujúce časti, resp. typy spracovania osobných údajov podľa účelu spracovania:
 - Kategória dotknutých osôb, ktorých sa spracúvanie týka (napr. klienti, potenciálni klienti).
 - Právne tituly ku každému spracúvaniu (napr. so súhlasom dotknutých osôb)
 - Dĺžka spracúvania osobných údajov v závislosti na účele spracúvania.
 - Uplatňovanie práv dotknutých osôb (napr. právo na prístup k osobným údajom).
 - Spôsob archivácie a následná likvidácia osobných údajov.
 - Podmienky, za ktorých sú údaje odovzdávané alebo sprístupňované tretím osobám.
 - Ak áno, ako je nakladanie s údajmi právne ošetrené?
 - Popis jednotlivých informačných systémov spracovávajúcich osobné údaje a ich previazanosť.
 - Zoznam všetkých povinností vo vzťahu k ochrane osobných údajov pre všetkých v rámci celej firmy (bude sa týkať napr. personálneho oddelenia, marketingu, finančného a mzdového oddelenia, oddelenia podpory, klientských služieb, oddelenia starostlivosti o zákazníka, administratívnej podpory, IT, vývoja produktu, výskumu)
 - Zásady zabezpečenia osobných údajov vo vzťahu k príslušnej agende.
2. **Zoznam všetkých existujúcich povinností**
3. **Zoznam zodpovedností jednotlivých osôb vo vzťahu k povinnostiam**
4. **Zoznam všetkých úloh**

4.3. IT systém

Keď si na správu osobných údajov zvolíte spoľahlivý informačný systém, máte na pol vyhraté – umožní vám definovať role a prístupové práva užívateľov, sledovať jednotlivé agendy i typy spracúvania údajov i oveľa viac. V rámci príprav na GDPR vám toho veľa zjednoduší:

- načítat' údaje z aplikácií a tie ďalej podľa nastavených procesov spracovať,
- definovať hlásenia a procesy na základe rolí, skupín a organizačnej štruktúry,
- všetky dokumenty je možné archivovať a zabezpečiť elektronickým podpisom,
- k dokumentom je možné na konci procesu vytvárať súhrnnú správu,
- definovať role, skupiny, organizačnú štruktúru,
- v rámci číselníkov je možné sledovať jednotlivé agendy i typy spracúvania,
- prípadne údaje regulátorovi odosielať priamo cez dátovú schránku.



S čím vám pomôže ekonomický systém POHODA sa dozviete v nasledujúcich kapitolách.

4.4. Zoznam nových povinností

V tomto kroku by ste už mali mať v ruke všetky dokumenty, ktoré analyzujú aktuálny stav nakladania s osobnými údajmi vo vašej firme. Teraz je čas na to, aby ste ich porovnali s tým, čo od vás žiada GDPR.

Posúdenie vplyvu na ochranu osobných údajov

Nariadenie GDPR (konkrétne článok 35) hovorí o tzv. Data Protection Impact Assessment (DPIA), čo predstavuje nástroj, ktorý pomáha organizáciám posúdiť vplyv na ochranu osobných údajov a identifikovať najefektívnejší spôsob, akým uviesť interné pravidlá do súladu s GDPR. Vy tak musíte vyhodnotiť, či máte povinnosť DPIA dokumentáciu vypracovať.

- DPIA sa povinne vykonáva:
 - pri systematickom a rozsiahlom hodnotení osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní (vrátane profilovania),
 - pri rozsiahlom spracúvaní citlivých osobných údajov,
 - pri rozsiahlom systematickom monitorovaní verejne prístupných miest,
 - ďalšie prípady, kedy je vykonanie DPIA povinné, môže určiť dozorný orgán.
- DPIA musí obsahovať aspoň:
 - opis plánovaného spracúvania, účely a oprávnené záujmy,
 - posúdenie nutnosti a primeranosti spracúvania vo vzťahu k účelu,
 - posúdenie rizika pre práva a slobody dotknutých osôb,
 - plánované opatrenia na odstránenie alebo zníženie týchto rizík.

Z výsledkov analýzy DPIA môže vyplynúť, že niektoré riziká nie je možné eliminovať alebo ich znížiť. V prípade kontroly dozorného orgánu tak budete môcť všetko potrebné doložiť práve vďaka tejto dokumentácii.

Získanie súhlasu so spracúvaním osobných údajov

Nie je pravdou, že pre každé spracovanie osobného údaja je potrebný súhlas. Nepotrebuje ho a ani by ste ho po dotknutej osobe nemali vyžadovať v prípadoch, kedy:

- spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy,
- spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa,
- spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby,
- spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi,
- spracúvanie je nevyhnutné pre účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä detí.

Ak spracúvate údaje z iných ako vyššie uvedených dôvodov, súhlas už preukázať musíte. Musí byť teda zaznamenaný preukázateľne a musí byť v prípade potreby dokladovateľný, v tomto ohľade nie je problém ho mať e-mailom. Ďalej súhlas musí byť dobrovoľný, nie je možné ním podmieniť čerpanie nejakej služby. Musí byť tiež jednoznačný v účele a rozsahu, musí byť oddelený napríklad od obchodných podmienok, nesmie byť schovaný v zmluvách apod. Musí byť tiež konkrétne stanovené na aký účel je poskytnutý, napríklad na účel zasielania obchodných informácií. A v neposlednom rade musí byť súhlas informovaný, t.j. musí byť jasné, komu je súhlas udelený, že sa neodovzdáva mimo EÚ a ako je možné ho odvolať.

Zodpovedná osoba

Úlohu zodpovednej osoby pre ochranu osobných údajov sme vysvetlili už v rámci základných GDPR pojmov. Preto len pripomíname, že niektoré firmy či organizácie takúto osobu sú povinné mať.

Revízia interných pravidiel aj uzatvorených zmlúv

Veľa osobných údajov spravujete na základe zmluvného vzťahu, zrevidujte či aktualizujte všetky dodávateľské zmluvy. Nezabudnite ani na svojich zamestnancov – poučte ich o zásadách GDPR a preškoľte ich v nastavených interných pravidlách.

Práva dotknutej osoby

Právo na opravu

Každý subjekt má podľa nariadenia GDPR právo požiadať o opravu nepresných údajov, ktoré o ňom evidujete.

Právo na vymazanie

Dotknutá osoba má právo na vymazanie osobných údajov zo strany prevádzkovateľa, ak je daný jeden z nariadenia vymenovaných dôvodov, medzi ktoré patrí:

- osobné údaje už nie sú potrebné pre účely, pre ktoré boli spracúvané,
- dotknutá osoba odvolala svoj súhlas alebo namieta voči spracúvaniu osobných údajov,
- osobné údaje boli spracúvané protiprávne.

Právo na obmedzenie spracúvania

Dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie, pokiaľ ide o jeden z týchto prípadov:

- dotknutá osoba napadne správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov dotknutej osoby,
- spracúvanie je protizákonné a dotknutá osoba namieta proti vymazaniu osobných údajov, ale žiada namiesto toho obmedzenie ich použitia,
- prevádzkovateľ už nepotrebuje osobné údaje na účely spracúvania (a mal by ich zmazať), ale potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov,
- dotknutá osoba namieta voči spracúvaniu a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevážujú nad oprávnenými dôvodmi dotknutej osoby.

4.5. Analýza rizík

Ak ste správne vykonali všetky predchádzajúce kroky, máte k dispozícii potrebné podklady pre vyhodnotenie rizikových oblastí. Táto analýza by mala obsahovať aspoň nasledujúce prvky:

- 1. Popis posudzovanej aktivity** – definícia, účel, charakteristika
- 2. Klasifikáciu rizika (nízke/stredné/vysoké)**
 - Vysoké riziko zakladá napr. povinnosť vykonať hodnotenie vplyvu na ochranu osobných údajov (DPIA, podľa článku 35 GDPR) alebo povinnosť predchádzajúcej konzultácie s dozorným orgánom (podľa článku 36 GDPR).
 - Vysoko rizikovým je napr. spracúvanie, ktoré využíva nové technológie a kde je pre dotknutú osobu práčne uplatniť svoje práva.
 - Nízke riziko naopak pripúšťa niektoré výnimky z povinností, napr. z povinnosti oznamovať porušenie zabezpečenia dozornému orgánu (podľa článku 33 GDPR).
- 3. Pravdepodobnosť vzniku škody**
 - Pravdepodobnosť stúpa napr. s počtom osôb zapojených do spracúvania osobných údajov a so zapojením tretích strán, pravdepodobnosť môže zvýšiť tiež história predchádzajúcich incidentov, kedy ku vzniku škody došlo.
- 4. Klasifikáciu možnej škody (malá/stredná/veľká)**
 - Závažnosť možnej škody je daná najmä mierou citlivosti údajov, objemom spracúvaných osobných údajov, mierou zraniteľnosti dotyknej osoby alebo mierou dopadu na ekonomické a spoločenské pomery dotyknej osoby.
- 5. Typizáciu škody**
 - Materiálna (napr. škoda na majetku zneužitím platobných údajov)
 - Nemateriálna (napr. poškodenie dobrého mena, zneužitie identity)
 - Spoločenská (napr. diskriminácia)
- 6. Identifikáciu prípadného sektorovo-špecifického rizika**
 - Hodnotenie vzťahu rizika a prínosu spracúvania osobných údajov
 - Prínos organizácii (napr. možnosť implementovať riešenie)
 - Prínos spoločnosti (napr. verejný záujem)
 - Prínos jednotlivcovi (napr. možnosť čerpať požadovanú službu)
- 7. Posúdenie prípadných globálnych súvislostí v prípade nadnárodných spoločností**

4.6. Opatrenia na odstránenie rizík

Posledným krokom sú opatrenia, ktoré vo firme nastavíte, aby ste všetkým rizikám z vykonanej analýzy predišli alebo ich odstránili.

Opatrenia na odstránenie rizík môžu napríklad spočívať v nasledujúcich činnostiach:

1. Zamestnanci budú preškolení o GDPR a s ním súvisiacimi novými povinnosťami (napríklad povinnosť doložiť súhlas dotknutej osoby so spracúvaním osobných údajov). Účast' na školení bude dokladovaná a/alebo sa zamestnanci podpisom zaviazajú dodržiavať interné pravidlá týkajúce sa ochrany osobných údajov.
2. Obmedzíte počet osôb, ktoré majú k osobným údajom prístup, na tých zamestnancov, ktorí s údajmi skutočne pracovať musia. O zmluvných partneroch a ďalších stranách nehovoriac.
3. Prístup k osobným údajom bude zabezpečený i fyzicky či technicky. Už žiadne počítače bez hesla, heslá nalepené na monitoroch, voľné prenášanie osobných údajov na akomkoľvek nosiči von z firmy alebo odomknutá voľne prístupná kartotéka, ani ukladanie dokumentov obsahujúcich osobné údaje na nezaistených verejných online úložiskách.
4. IT oddelenie alebo správca IT siete upraví bezpečnostné procesy tak, aby minimalizovali možnosti úniku osobných údajov.
5. Zlikvidujete osobné údaje, na uchovanie ktorých už neexistuje oprávnený dôvod.
6. Údaje, ktoré je možné anonymizovať, anonymizujete.

5. Správa osobných údajov v programe POHODA

Na správu osobných údajov v programe POHODA je najvhodnejšia agenda Adresár. Keďže do nej ukladáte všetky kontaktné a fakturačné údaje zákazníkov či dodávateľov, je ideálne, keď budete na rovnakom mieste spravovať i všetko potrebné podľa nariadenia GDPR. Konkrétne odkedy, dokedy a prečo máte údaje v evidencii, ako sa účely ich spracovania časom menili alebo napríklad kto s údajmi pracuje. Funkčnosť pre GDPR je potrebné najskôr aktivovať v agende Globálne nastavenie/GDPR zaškrtnutím voľby Povolit GDPR.

V agende Adresár sa sprístupní záložka GDPR, na ktorej si jednoducho vyberiete účel spracúvania údajov v stĺpci Názov, podľa ktorého POHODA automaticky doplní popis dôvodu, a potrebné dáta spracúvania. POHODA vám dôvody spracúvania sama ponúkne, do zoznamu si ale samozrejme môžete pridať i vlastné. Ako na to sa dozviete hneď v nasledujúcej kapitole.

Záložka GDPR v agende Adresár obsahuje, z pohľadu správy osobných údajov, jednu užitočnú funkciu, z ktorej sa dá zistiť, kedy naposledy ste danú adresu použili na predpredajných, predajných a popredajných dokladoch:

Predpredajné doklady – Prijaté ponuky, Vydané ponuky, Prijaté dopyty, Vydané dopyty

Predajné doklady – Banka, Pokladňa, Interné doklady, Prijaté objednávky, Vydané objednávky, Vydané faktúry, Vydané zálohové faktúry, Ostatné pohľadávky, Prijaté faktúry, Prijaté zálohové faktúry, Ostatné záväzky, Predajky

Popredajné doklady – Reklamácie, Servis

Z pohľadu nariadenia GDPR sa tak oplatí všetko (od vydanej ponuky až po reklamačný protokol) evidovať priamo v ekonomickom systéme POHODA, jedine tak budete mať dokonalý prehľad o spracúvaní osobných údajov. Dobu, počas ktorej je pre vás vystavenie jednotlivých typov dokladov dôvodom na spracúvanie osobných údajov obchodných partnerov, si môžete nastaviť v agende Globálne nastavenie/GDPR.

5.1. Vyhľadanie, úprava a vymazanie osobných údajov

Každý subjekt má podľa nariadenia GDPR právo požiadať o opravu alebo vymazanie údajov, ktoré o ňom evidujete. Vďaka programu POHODA údaje rýchlo vyhľadáte, upravíte, ale i vymažete.

TIP Práci so záznamami sa venuje 7. diel e-learningového kurzu [POHODA – školenie základných vedomostí](#).

V ponuke Záznam/GDPR agendy Adresár nájdete navyše vychytávky na hromadné vyplnenie záložky GDPR pri viacerých adresách naraz (povel Hromadne pridať dôvod spracúvania ...) a na výber adres s aktuálne platným súhlasom či účelom alebo naopak s končiacim súhlasom k určitému dátumu (povel Vyhľadať záznamy...) Možností vyhľadávania adres podľa právnych dôvodov spracúvania je hneď niekoľko, POHODA rozlišuje:

1. Platné dôvody
2. Dôvody s končiacou platnosťou
3. Exspirované dôvody
4. Adresy bez dôvodu spracúvania

Podľa zvolenej možnosti sa na druhej strane sprievodcu zobrazia rozšírené voľby pre vyhľadanie. V prípade bodu 1–3 je možné vyhľadať:

- **Všetky dôvody** – POHODA vyberie adresy, pri ktorých je zadaný aspoň jeden právny dôvod, a zároveň sú všetky zadané dôvody platné.
- **Akýkoľvek dôvod** – POHODA vyhľadá adresy, pri ktorých existuje aspoň jeden právny dôvod, ktorý je zároveň platný.
- **Niektorý z vybraných** – POHODA umožní v ďalšom poli pomocou výklopného zoznamu vybrať konkrétne právne dôvody. Následne vyhľadá adresy, pri ktorých je aspoň jeden z týchto vybraných dôvodov platný.
- **Všetky vybrané** – táto možnosť je podobná ako pri predchádzajúcej voľbe, tentokrát však musia byť pri zázname všetky vybrané dôvody vyplnené a všetky musia byť platné.

i Rozdiel medzi voľbami **Všetky** a **Všetky vybrané** spočíva okrem iného v tom, že voľba **Všetky** zohľadňuje iba dôvody v adrese skutočne zadané. Pri voľbe **Všetky vybrané** sa požaduje, aby adresa skutočne obsahovala všetky vybrané dôvody, inak do filtra nevstúpi.

Vyhľadanie adres podľa práv. dôvodov pre spracúvanie osob. údajov

Vyhľadanie adres podľa práv. dôvodov pre spracúvanie osob. údajov

Táto funkcia vám umožní vybrať záznamy v agende Adresár na základe právnych dôvodov pre spracúvanie osobných údajov zadaných v záložke GDPR.

Vyberte jednu z ponúkaných možností i podľa toho, aké záznamy hľadáte.

Platné
Vyhľadá záznamy, ktoré majú zvolené právne dôvody stále platné.

S končiacou platnosťou
Umožní vybrať záznamy, ktorým v zadanom časovom období končí platnosť právnych dôvodov.

Exspirované
Vyhľadá záznamy, ktorým už vypršala platnosť vybraných právnych dôvodov.

Bez dôvodu spracúvania
Vyberie adresy, ktorým nie sú evidované konkrétne právne dôvody.

< Naspäť **Ďalej >** Stomo Pomocník

Vyhľadanie adres podľa práv. dôvodov pre spracúvanie osob. údajov

Vyhľadanie adres podľa práv. dôvodov pre spracúvanie osob. údajov
S končiacou platnosťou

Táto strana sprievodcu slúži na výber adres, ktorým v zadanom období končí platnosť jedného či viac právnych dôvodov.

Vybrať adresy, ktorým končí platnosť do:

Všetky vybrané

Vybrané právne dôvody:

Voľte či môžete zahnúť aj dôvody vyplývajúce z existujúcich dokladov:

Predpredajné doklady mesiace

Predajné doklady mesiace

Popredajné doklady neobmedzené

< Naspäť **Dokončiť** Stomo Pomocník

i Iba v prípade hľadania exspirovaných adries máte k dispozícii voľbu **Vrátane adries bez vyplneného dôvodu**. Ak teda pri adrese nie je zadaný dôvod, berie sa adresa na účely hľadania rovnako, ako by bol dôvod exspirovaný.

V prípade poslednej možnosti, teda adries bez dôvodu spracúvania, je možné vyhľadať:

- **Žiadny dôvod** – POHODA vyberie adresy, pri ktorých nie je zadaný žiadny dôvod spracúvania.
- **Niektorý z vybraných dôvodov** – POHODA vyhľadá adresy, pri ktorých chýba aspoň jeden z vybraných dôvodov.
- **Žiadny z vybraných dôvodov** – POHODA vyhľadá adresy, u ktorých nie je ani jeden z vybraných dôvodov.

Vyhľadanie adries podľa práv. dôvodov pre spracúvanie osob. údajov

Vyhľadanie adries podľa práv. dôvodov pre spracúvanie osob. údajov
Bez dôvodu spracúvania

Táto funkcia vám umožní vybrať záznamy v agende Adresár, ktoré nemajú v záložke GDPR evidovaný žiadny právny dôvod pre spracúvanie osobných údajov.

Vybrať adresy, ktoré nemajú zadaný právny dôvod:
Žiadny z vybraných

Vybrané právne dôvody:

Voliteľne môžete zahrnúť aj dôvody vyplývajúce z existujúcich dokladov:

Predpredajné doklady
 Predajné doklady
 Popredajné doklady

< Naspäť **Dokončiť** Stomo Pomocník

Vo všetkých možnostiach vyhľadávania (1–4) potom môžete voľiteľne zahrnúť tiež dôvody vyplývajúce z vystavených dokladov – predpredajných, predajných a popredajných.

Vyhľadanie adries podľa práv. dôvodov pre spracúvanie osob. údajov

Vyhľadanie adries podľa práv. dôvodov pre spracúvanie osob. údajov
Platné

Na tejto strane môžete vybrať právne dôvody pre spracúvanie osobných údajov. Po stlačení tlačidla **Dokončiť** budú vyfiltrované adresy, pri ktorých sú tieto dôvody zadané v záložke GDPR a sú stále platné.

Vybrať adresy obsahujúce platný právny dôvod:
Všetky vybrané

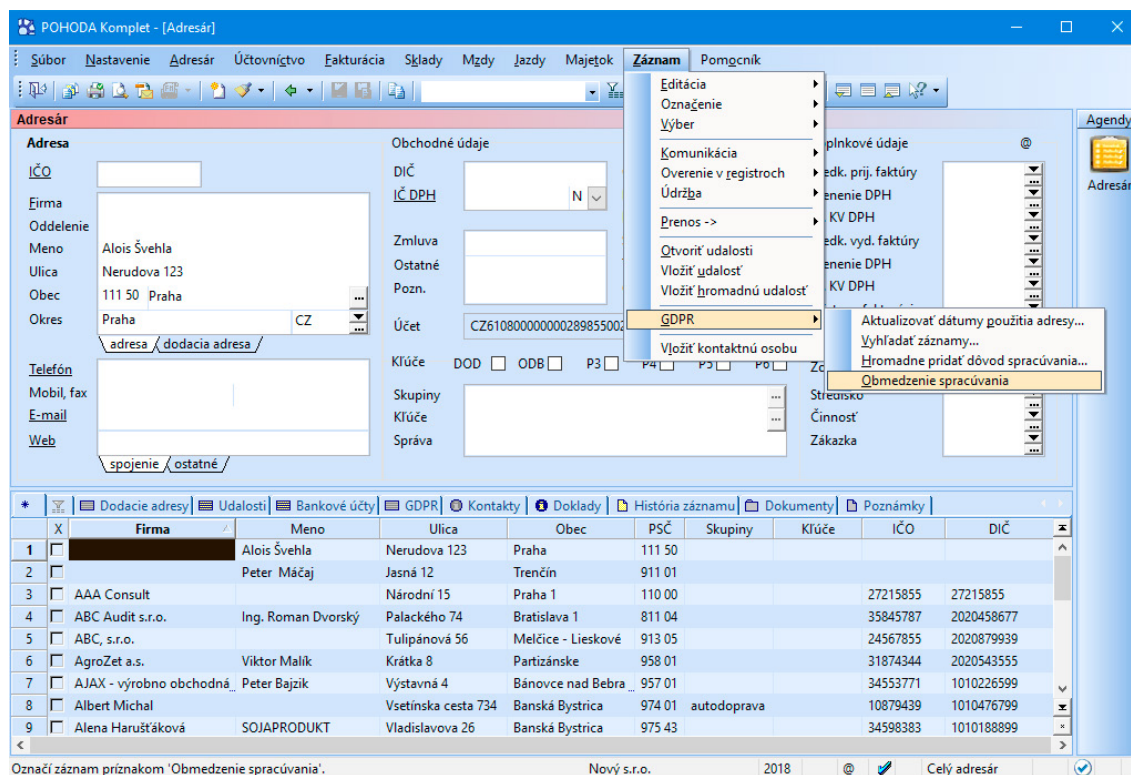
Vybrané právne dôvody:

Voliteľne môžete zahrnúť aj dôvody vyplývajúce z existujúcich dokladov:

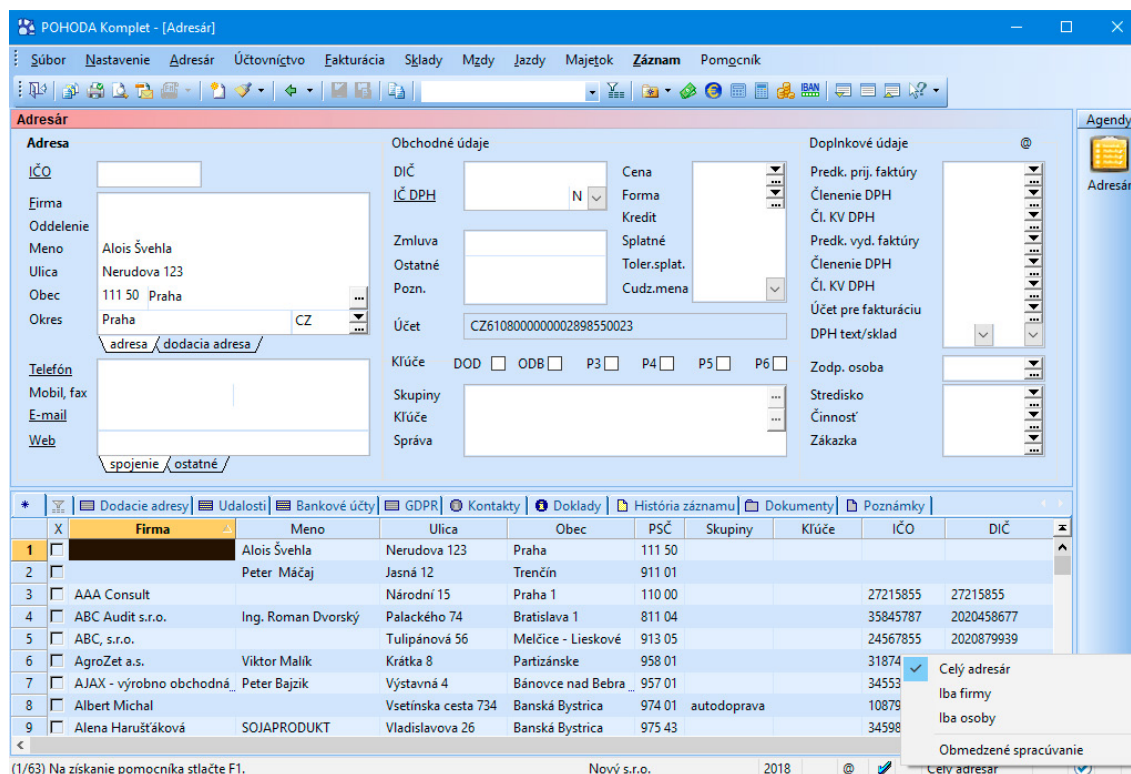
Predpredajné doklady 3 mesiace
 Predajné doklady 24 mesiace
 Popredajné doklady neobmedzené

< Naspäť **Dokončiť** Stomo Pomocník

POHODA vám umožní konkrétnu adresu označiť príznakom Obmedzené spracúvanie, ktorý zaistí, aby adresa nebola pre užívateľa programu viditeľná, a znepřístupní ju na ďalšie použitie. Ide o umožnenie realizácie práva dotknutej osoby na obmedzenie spracúvania podľa článku 18 Všeobecného nariadenia o ochrane osobných údajov.

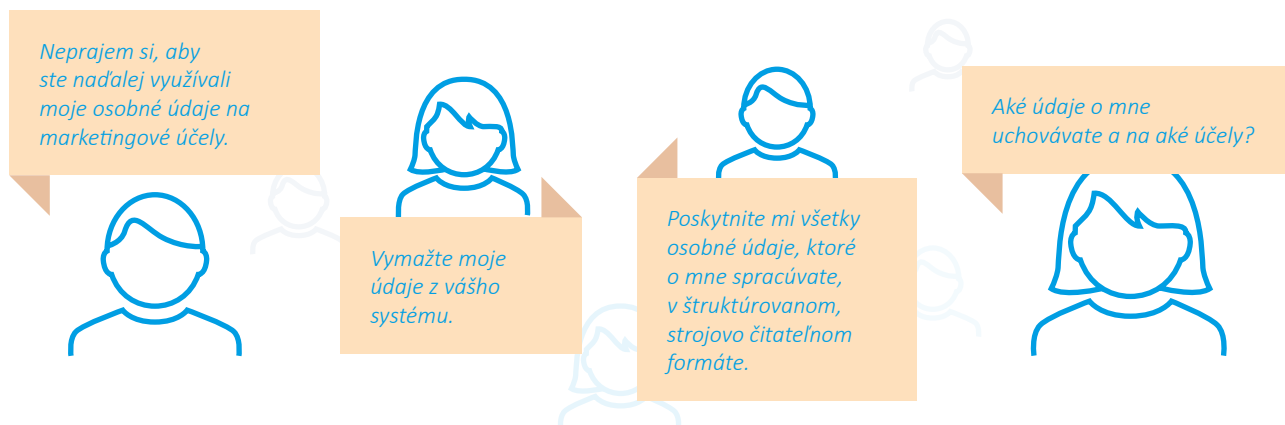


Všetky adresy, ktorým ste priradili príznak Obmedzené spracúvanie, si zobrazíte iba kliknutím pravého tlačidla myši na stavovom riadku v časti, kde sa volí rozsah zobrazenia záznamov a zvolením možnosti Obmedzené spracúvanie.



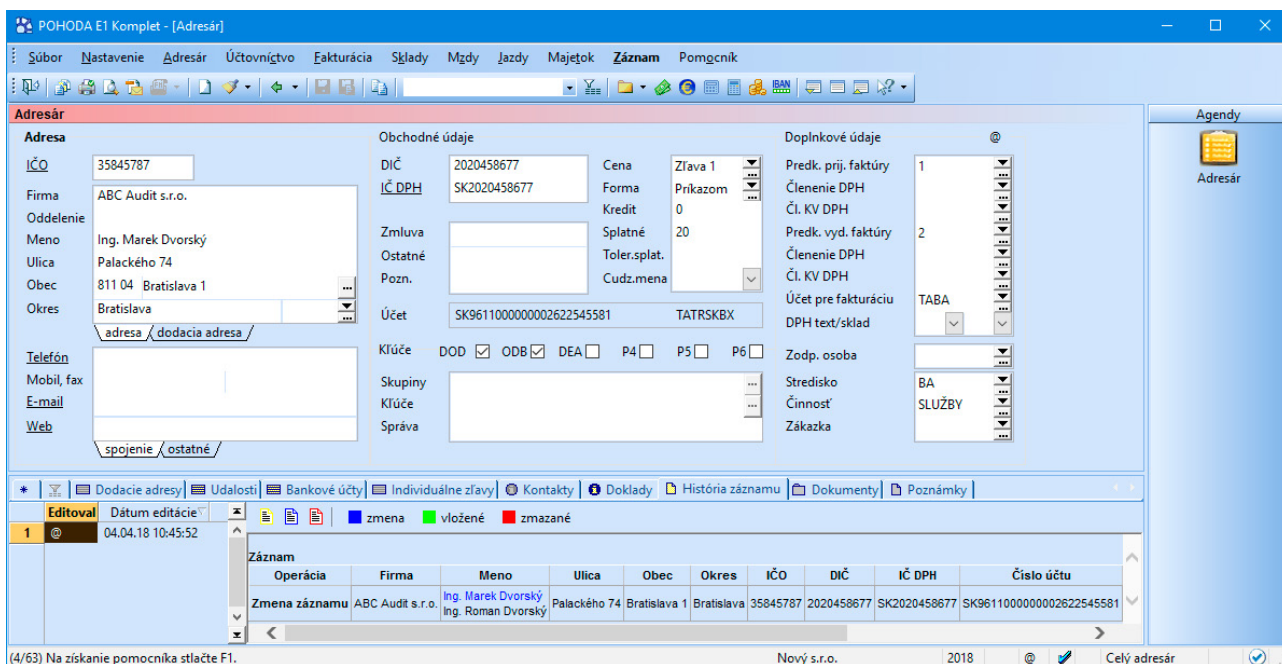
S programom POHODA tak budete vždy schopní reagovať na požiadavky dotknutých osôb:

- Vymažte moje údaje z vášho systému.
- Poskytnite mi všetky osobné údaje, ktoré o mne spracúvate, v štruktúrovanom, strojovo čitateľnom formáte.
- Neprajem si, aby ste naďalej využívali moje osobné údaje na marketingové účely.
- Aké údaje o mne uchováвате a na aké účely?



5.2. História záznamov

Jednoducho skontrolujete, kedy a kto z užívateľov programu s údajmi manipuloval. Ak sa opraví údaj, POHODA uloží jeho pôvodnú verziu automaticky na záložku História záznamu. Vymazané, zmenené a novo vložené údaje sú na záložke kvôli lepšej prehľadnosti farebne označené.

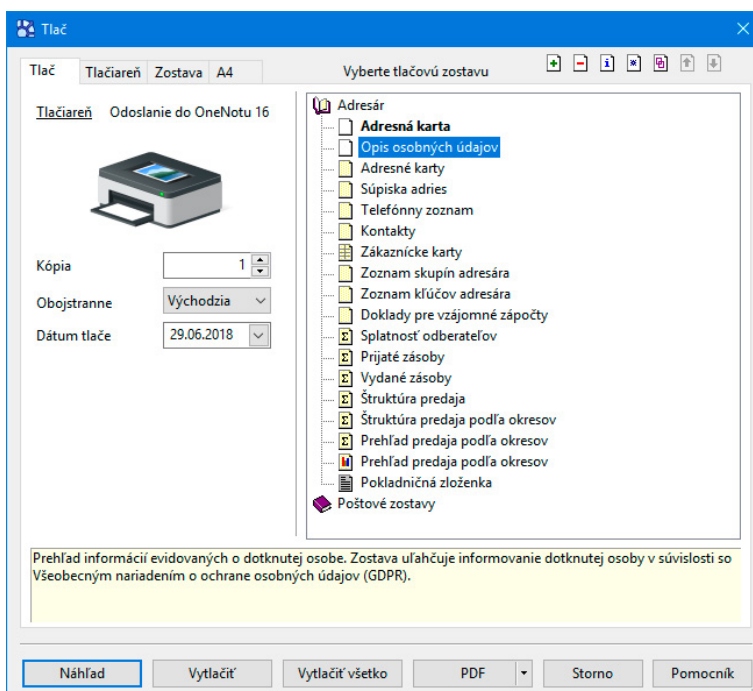


Históriu zmien v jednotlivých agendách si jednoducho zapnete v agende Globálne nastavenie, a to prostredníctvom voľby Evidovať históriu zmien. Táto funkčnosť je pre väčšinu agend dostupná vo všetkých produktových radoch programu POHODA a na účely GDPR ju využijete v agende Adresár.

5.3. Súpiska s údajmi vybranej dotknutej osoby

Ak vás niekto požiada o predloženie uceleného súhrnu jeho osobných údajov, jednoducho si vygenerujete tlačovú zostavu Opis osobných údajov priamo z agendy Adresár, ktorá vám tento súpis poskytne (zostava so spracúvanými údajmi sa vám bude hodiť pri prípadnej kontrole). S programom POHODA tak budete vždy schopní reagovať na práva dotknutej osoby podľa článku 15 nariadenia GDPR.

Ak je vo vašej organizácii menovaná zodpovedná osoba pre ochranu osobných údajov, môžete údaje o nej zadať v agende Globálne nastavenie/GDPR, a bude sa tlačiť na zostave Opis osobných údajov.

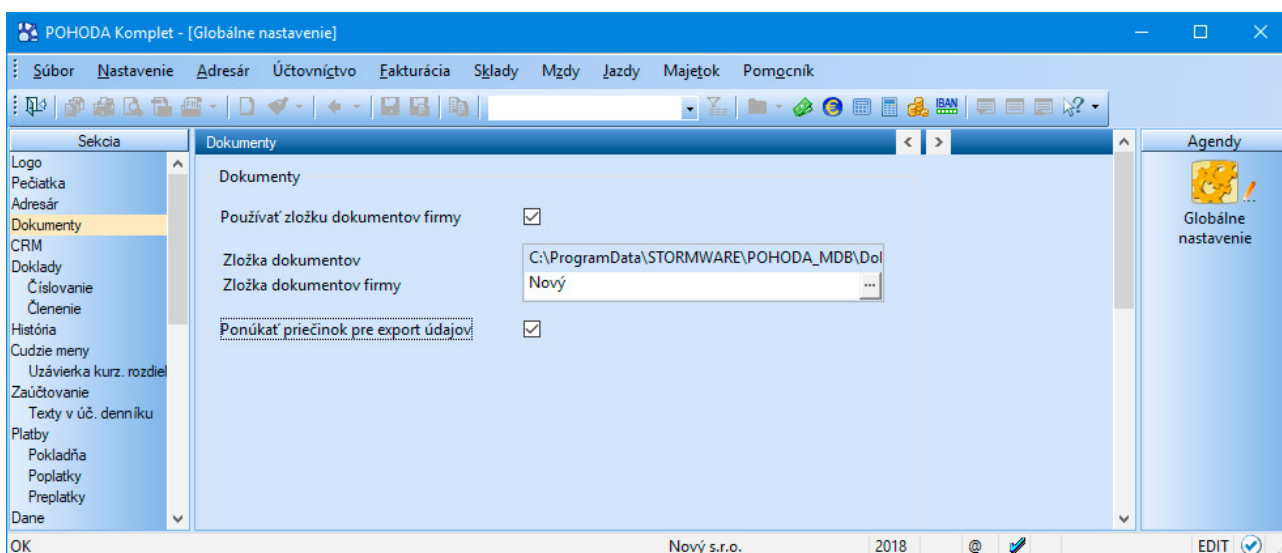


5.4. Práca s dokumentami

Všetky svoje listy, zmluvy, tabuľky a akékoľvek ďalšie dôležité dokumenty si môžete v programe POHODA prehľadne usporiadať. Lahko ich priradíte k adresám i k udalostiam a pristupovať k nim môžete nielen z programu Prieskumník v Microsoft Windows, ale tiež z vybraných agend. Z hľadiska nariadenia GDPR je to ideálna cesta, ako mať priamo pri danom kontakte – osobnom údajy priložené všetky dôležité dokumenty či súhlasy.

Vôbec prvým krokom je nastavenie priečinka, do ktorého sa budú všetky dokumenty ukladať. V agende **Globálne nastavenie v sekcii Dokumenty** najskôr zaškrtníte možnosť Používať zložku dokumentov firmy. Potom si všimnete tieto polia:

- **Zložka dokumentov** – v tomto poli sa automaticky ponúkne cesta k adresáru vo vašom počítači. Ide o údajový priečnik programu POHODA, ktorý sa založil automaticky v priebehu inštalácie programu. Odporúčame toto umiestnenie nemeniť.
- **Zložka dokumentov firmy** – do tohto políčka POHODA automaticky doplní názov vytváraného priečinka, ktorý bude pomenovaný ako účtovná jednotka, v ktorej toto nastavenie vykonávate. Ak chcete priečnik nazvať inak, jednoducho do neho kliknite a prepíšete ho. (Názov nového priečinka/zložky v tomto poli je automaticky skratený o doplnky typu s.r.o., a.s. a pod.)

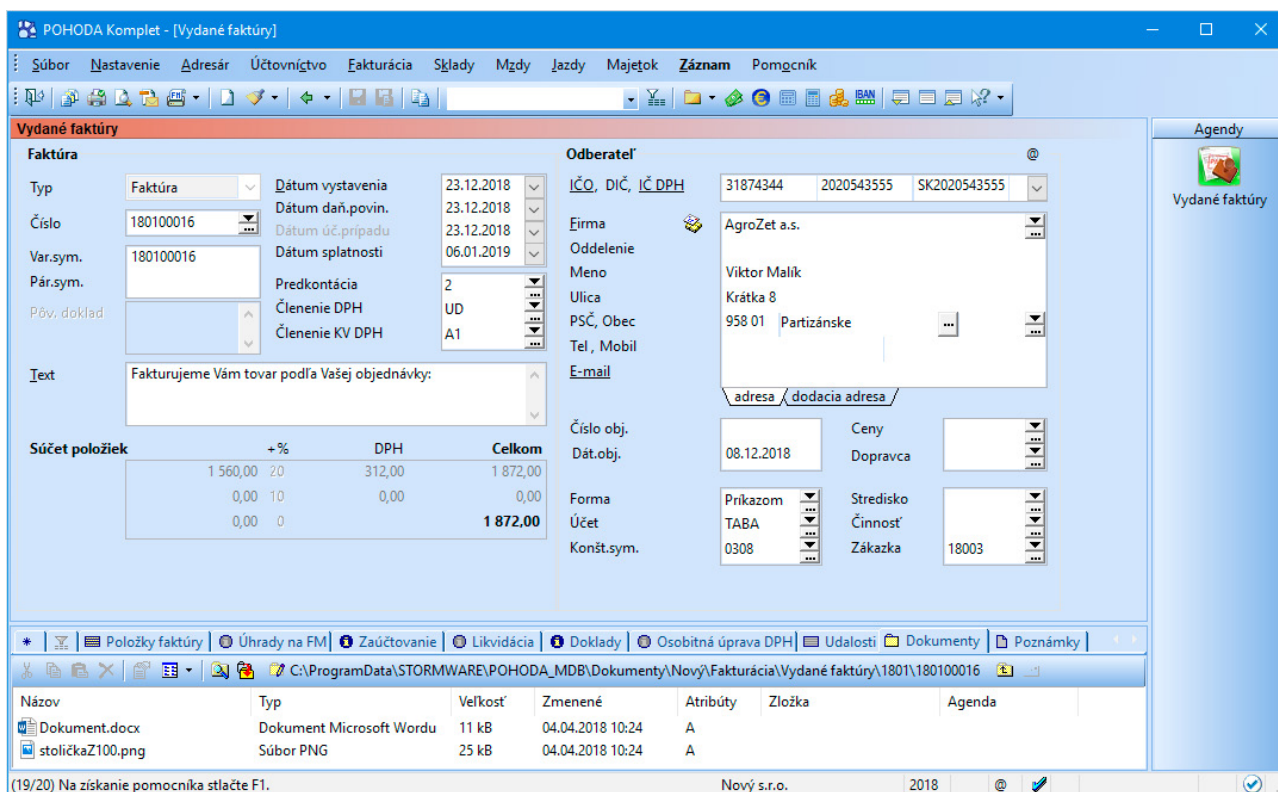


Na prácu so súbormi slúži ponuka povelov a tlačidiel. V agende Adresár vyberte záznam, ku ktorému chcete priradiť dokumenty. Najskôr tu kliknite na tlačidlo <<**Priečnik nie je definovaný**>>. POHODA zobrazí dialógové okno, v ktorom rovno ponúkne umiestnenie a vytvorenie priečinka pre daný záznam.










K vybranému záznamu v agende Adresár vložíte súbor pomocou tlačidla **Začleniť súbory**. Otvorí sa okno, z ktorého obvyklým spôsobom vyhladáte súbor zo svojho počítača. Vo výklopnom zozname môžete vybrať, akým spôsobom sa má súbor preniesť, a to:

- **kopírovať** – vkladajúci súbor zostane na pôvodnom mieste a jeho kópie sa vložia do nadefinovaného priečinka pre dokumenty (táto možnosť je v dialógovom okne nastavená ako východisková),
- **vytvoriť zástupcu** – súbor zostane stále na pôvodnom mieste a z programu POHODA sa naň budete iba odkazovať,
- **presunúť** – súbor sa z pôvodného umiestnenia presunie do nadefinovaného priečinka.

Hneď ako niektorú z týchto troch operácií zvolíte, vybraný súbor sa objaví pri danom zázname na záložke Dokumenty programu POHODA.



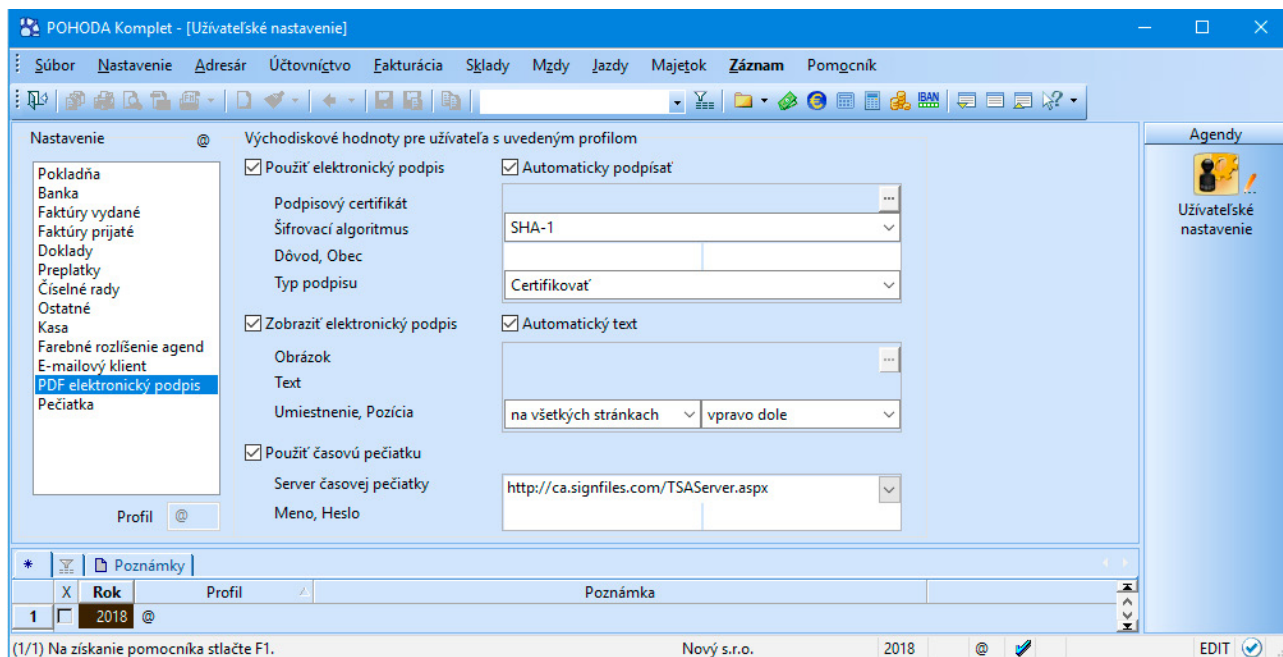
Ak na nejaký súbor na záložke Dokumenty kliknete, aktivujú sa ďalšie tlačidlá na prácu so súborom:

-    – tlačidlá na vystrihnutie, kopírovanie a vloženie súboru do zložky/priečinka
-  – tlačidlo na vymazanie súboru zo zložky dokumentov
-  – tlačidlo na nastavenie vlastností súboru
-  – tlačidlo, ktorým ovplyvníte zobrazenie súborov v zložke dokumentov
-  – tlačidlo na otvorenie zložky dokumentov v aplikácii Prieskumník
-  – tlačidlo na vytvorenie alebo premenovanie zložky
-  – tlačidlo na odoslanie dokumentu e-mailom

5.5. Podpisovanie PDF dokumentov

Doteraz bola reč predovšetkým o dokumentoch, ktoré do programu POHODA k jednotlivým záznamom priradujeme z externých úložísk, za účelom prehľadnejšieho spravovania osobných údajov. Teraz niečo o dokumentoch vygenerovaných z programu POHODA. Podľa nariadenia GDPR totiž musíte vedieť, kto osobné údaje akokoľvek spracovával – tým sa samozrejme myslí i generovanie PDF dokumentov, ktorých súčasťou tieto osobné údaje sú. Ako teda zistíte, kedy a kto vytvoril konkrétny PDF dokument z programu POHODA? Jednoducho, stačí konkrétnemu užívateľovi nastaviť časovú pečiatku a elektronický podpis priamo v agende Užívateľské nastavenie.

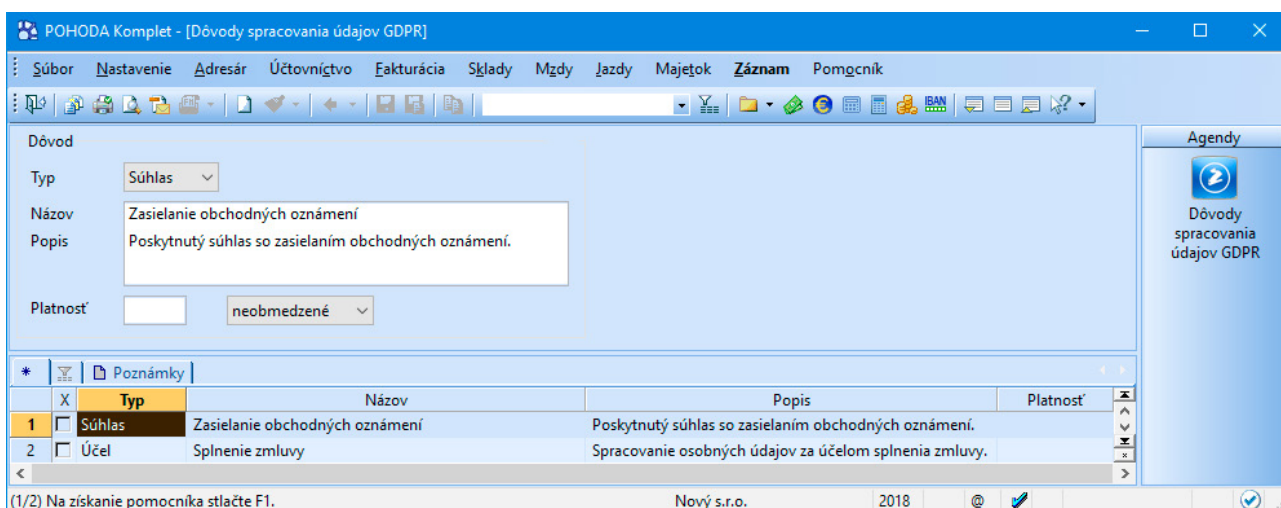
Po zaškrtnutí voľby Použiť elektronický podpis v sekcii PDF elektronický podpis vyberte šifrovací algoritmus, typ podpisu, podpisový certifikát a zadajte údaje, ktoré sa budú zobrazovať vo vlastnostiach podpisu vytvoreného PDF dokumentu. Ak zaškrtnete voľbu Zobrazit' elektronický podpis, bude automaticky nastavený východiskový obrázok a text podpisu. Text aj obrázok podpisu si môžete zvoliť podľa seba. Pri použití časovej pečiatky si môžete vybrať server na overovanie časového okamihu, pred ktorým dokument zaručene existoval. Časová pečiatka obsahuje predovšetkým aktuálny dátum a čas, sériové číslo pečiatky a identifikáciu autority, ktorá túto pečiatku vydáva. Pre prístup na server je dôležité zadať meno a heslo užívateľa.



Všetky údaje, ktoré na podpisovanie PDF dokumentov zadáte v agende Užívateľské nastavenie, môžete dodatočne alebo operatívne zmeniť v dialógovom okne Elektronické podpísanie PDF, ktoré sa zobrazuje pri vytváraní PDF dokumentu.

6. Dôvody spracúvania osobných údajov

POHODA obsahuje špeciálnu agendu, v ktorej sú právne dôvody spracúvania osobných údajov už preddefinované. Agenda vám však poskytuje tiež maximálny priestor na zapísanie dôvodov vlastných – predsa len, každý obor podnikania zahŕňa špecifické služby, a tým pádom existuje veľa okolností spracúvania údajov. Pri zápise nového záznamu (dôvodu) stačí vyplniť preddefinované polia formulára. Tieto záznamy potom môžete priradovať k jednotlivým záznamom v agende Adresár. Agendu Dôvody spracúvania údajov GDPR nájdete v ponuke Nastavenie/Zoznamy.



Aké dôvody si do agendy programu POHODA zapíšete, je len na vás. Nezabúdajte však na zákonné dôvody, ktoré by mali predchádzať tým, pre ktoré potrebujete súhlas dotknutých osôb. Platná legislatíva napríklad nariaďuje podnikateľom, účtovným jednotkám a ďalším subjektom archivovať účtovné doklady, ktoré samozrejme veľakrát obsahujú údaje o zamestnancoch, spoločníkoch, obchodných partneroch alebo napríklad zákazníkoch. Pozrite sa na malý prehľad toho, aké dokumenty ste povinní uchovávať práve zo zákonného dôvodu. Archivačných lehôt a výnimočných situácií je však naozaj veľa, preto sa vždy musí brať do úvahy, o aký dokument sa jedná a aké preň v danej situácii platia lehoty úschovy.

Zákon č. 431/2002 Z. z. o účtovníctve definuje rôzne lehoty pri uchovávaní jednotlivých účtovných záznamov. Účtovná závierka, výkazy vybraných údajov z účtovných závierok a výročná správa sa uchovávali počas desiatich rokov nasledujúcich po roku, ktorého sa týkajú. Ďalej podľa zákona 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov (ďalej len zákon o archívoch a registratúrach) v znení novely č. 515/2003 Z. z. by ste mali postupovať nasledovne:

Archivácia dokladov do konca roka 2017:

Podľa starej legislatívy neboli jednotné archivačné obdobia na jednotlivé účtovné dokumenty a preto sa často stávalo, že daňový subjekt už archivovať účtovné doklady nemal, ale účtovnú závierku áno.

Účtovné doklady:

Neplatiteľ DPH:

Do roku 2017 neplatiteľ DPH musel archivovať účtovné doklady po dobu 5 rokov.

Platiteľ DPH:

Do konca roka 2017 mali povinnosť archivovať účtovné doklady po dobu 10 rokov.

Archivácia účtovných dokladov od 2018:

Počas 10 rokov nasledujúcich po roku, ktorého sa týkajú sa od roku 2018 archivujú:

účtovné doklady, účtovné knihy, zoznamy účtovných kníh, zoznamy číselných znakov alebo iných symbolov a skratiek použitých v účtovníctve, odpisový plán, inventúrne súpisy, inventarizačné zápisy a účtový rozvrh za rok.

Doba archivácie účtovných dokladov, ktoré sú podkladom na zostavenie účtovnej závierky, sa teda zosúladi s dobou archivácie účtovnej závierky. Taktiež bude zabezpečený súlad s daňovým poriadkom a doklady budú k dispozícii až do zániku práva na vyrubenie dane. Zákon o DPH vyžaduje rovnako uchovávanie faktúr po dobu 10 rokov.

Táto povinnosť sa netýka len nových dokladov po 1. 1. 2018. Povinnosť archivovať účtovné doklady 10 rokov platí pre všetky doklady, pri ktorých pôvodná päťročná doba uchovávaní ešte neuplynula. Zjednodušene povedané, účtovné doklady za rok 2012 je potrebné uchovávať do konca roka 2017. Na tieto doklady sa už novela nevzťahuje. Pokiaľ ale ide o účtovné doklady za rok 2013 (a neskôr), týmto uplynie päťročná lehota až v roku 2018, teda už je potrebné postupovať podľa nového znenia zákona o účtovníctve a archivovať je potrebné 10 rokov.

Zároveň sa nová lehota uchovávaní desať rokov vzťahuje aj na tie záznamy, ktoré sa týkajú spôsobu a formy vedenia účtovníctva (programové vybavenie, nosiče informácií na CD a pod.).

Účtovná jednotka môže archivovať účtovné záznamy v písomnej alebo elektronickej forme.

Archivácia mzdových dokladov:

Súčasťou registratúry je aj mzdová agenda. Mzdovú agendu tvoria písomnosti dokladujúce evidenciu, výpočet, zdaňovanie miezd a realizáciu zákonných a ostatných zrážok zo mzdy.

Sú to najmä:

- výplatná listina,
- mzdový list,
- evidenčný list dôchodkového poistenia,
- povinné výkazy o výške preddavkov na poistné pre jednotlivé zdravotné poisťovne a výške poistného a príspevkov pre Sociálnu poisťovňu,
- výkazy o zrazených preddavkoch na daň z príjmov fyzickej osoby a hlásenie o vyúčtovaní dane,
- rôzne potvrdenia o mzde.

Z hľadiska dokladovania identifikačných údajov zamestnanca, výpočtu a zdaňovania mzdy a pre účely dôchodkového zabezpečenia je **najdôležitejší ročný mzdový list**.

Zákon o účtovníctve ani iné predpisy neurčujú povinnú lehotu úschovy mzdových listov, je potrebné určiť ju v registratúrnom pláne. Podľa predchádzajúceho zákona o účtovníctve sa museli mzdové listy archivovať desať rokov a údaje z nich na dôchodkové zabezpečenie dvadsať rokov po roku, ktorého sa týkali. Je nevyhnutné, aby sa aj v súčasnosti stanovila lehota úschovy mzdových listov aspoň na minimálne dvadsať rokov nasledujúcich po roku, ktorého sa týkajú.

Lehotu úschovy dokladov potrebných na správne určenie vymeriavacieho základu a výšky preddavkov na poistné a poistné na zdravotné poistenie a poistné na nemocenské, dôchodkové poistenie a poistenie v nezamestnanosti je možné odvodiť od práva predpísať alebo vymáhať poistné, ktoré je v jednotlivých zákonoch stanovené takto:

10 rokov nasledujúcich po roku, ktorého sa týkajú	účtovné doklady, účtovné knihy, odpisový plán, inventúrne súpisy, inventarizačné zápisy
10 rokov nasledujúcich po roku, ktorého sa týkajú	doklady pre účely DPH
5 rokov po roku, ktorého sa týkajú	daňové doklady
10 rokov nasledujúcich po roku, ktorého sa týkajú	výplatné listiny a ostatná mzdová dokumentácia
10 rokov nasledujúcich po roku, ktorého sa týkajú	ročné mzdové listy
Minimálne 20 rokov nasledujúcich po roku, ktorého sa týkajú	osobné spisy







7. Bezpečnosť dát v programe POHODA

GDPR sa dotýka predovšetkým otázky ochrany súkromia a pre nás v STORMWARE je práve bezpečnosť dát prioritou č. 1. Stupeň zabezpečenia údajov spracúvaných v ekonomickom systéme POHODA závisí predovšetkým na použitej technológii, ktorá sa odlišuje v závislosti na produktovom rade programu – POHODA, POHODA SQL a POHODA E1.

7.1. Základný produktový rad POHODA

Základný produktový rad programu POHODA využíva technológiu file-server, čo znamená, že každý užívateľ pracuje s dátami, ktoré sú uložené priamo v jeho počítači (v prípade sieťového variantu potom na firemnom serveri). Samotné dáta sú zabezpečené pomocou overenia užívateľského hesla a systému základných prístupových práv. To znamená, že užívateľom môžete prideliť prístupové práva k jednotlivým agendám a funkciám.

A ako na to? V programe POHODA sa z ponuky Nastavenie otvorí agenda Prístupové práva/Užívateľia. Prístup má do nej iba administrátor (alebo užívateľ, ktorému priradil právo na vykonávanie tejto operácie). Na záložke Užívateľ vyberte toho, komu chcete práva zmeniť, a na záložke Práva zvolíte v stromovej štruktúre konkrétnu oblasť, napríklad Účtovníctvo, Mzdy alebo napríklad Prijaté faktúry. V sekcii Práva vo zvolenej úrovni potom už môžete užívateľovi nastaviť, aké operácie bude môcť so záznamami vykonávať. Pri práci v danej oblasti sa mu potom dole na príkazovom riadku zobrazí ikonka označujúca práve jeho oprávnenia:

-  **žiadne práva** – užívateľ nemá pre danú položku/agendu žiadne práva
-  **čítanie** – užívateľ má právo prehliadať záznamy, ale nemôže ich akokoľvek meniť alebo pridávať
-  **zápis** – užívateľ môže prehliadať záznamy a pridávať ďalšie
-  **zápis a modifikácia vlastných** – užívateľ má právo prehliadať záznamy, pridávať ďalšie, vlastné záznamy môže i meniť
-  **zápis a modifikácia všetkých** – užívateľ môže prehliadať, pridávať a meniť všetky záznamy
-  **všetky (vrátane mazania)** – užívateľ môže pridávať, prehliadať, meniť a vymazávať všetky záznamy

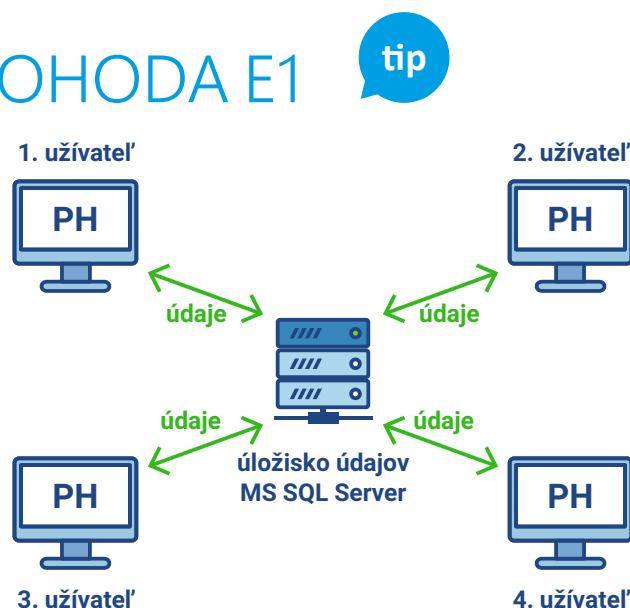
V programe POHODA môžete tiež sledovať históriu zmien, vo väčšine agend tak uvidíte, kto a kedy záznam vytvoril a uložil, stačí mať v Globálnom nastavení v sekcii História zaškrtnutú voľbu Evidovať históriu zmien. Ak navyše chcete zobraziť v agende i záložku História zmien, zaškrtnite voľbu Záložka. Jednotlivé záznamy je možné tiež zamknúť, aby nedochádzalo k nežiadúcim zásahom. Tento spôsob zabezpečenia je pre menšie firmy, ktoré pracujú s malým objemom dát, úplne postačujúci, program pracuje rýchlo a je bezpečný.

7.2. POHODA SQL a POHODA E1

tip

Pre väčšie firmy, ktoré spracovávajú veľa dát, sú vhodnejšie produktové rady POHODA SQL a E1, a to nielen kvôli rýchlosti a výkonu, ale i kvôli vyššiemu stupňu zabezpečenia dát. Využívajú totiž technológiu SQL. To znamená, že Vaše dáta sú uložené na zabezpečenom Microsoft SQL Serveri, kde je manipulácia s nimi dokumentovaná. SQL server má navyše k dispozícii administrátorské nástroje na správu systému, dát a sledovanie prevádzky databázového stroja.

Jednou z výhod radov POHODA SQL a E1 teda je, že užívateľia programu nemajú prístup priamo k zdrojovým dátam, tie sú uložené práve na SQL serveri. Po sieti sa prenášajú vždy iba tie záznamy, ktoré v danej chvíli užívateľ priamo potrebuje. Vaše citlivé dáta sú tak viac chránené proti poškodeniu a neoprávnenému prístupu alebo proti ich zneužitiu. Zároveň je tento prístup i rýchlejší, pri práci s veľkým množstvom dát alebo súbežnej práci viacerých užívateľov nedochádza k žiadnemu zdržiavaniu.



Užívateľia majú k dispozícii iba tie údaje, ktoré práve potrebujú

V produktových radoch POHODA SQL a E1 dokážete ešte svoje záznamy viacfázovo uzamknúť či využívať rozšírené prístupové práva, napr. na číselné rady či exporty agend. Tiež je možné určitým užívateľom obmedziť prístup k záznamom s vybranými číselnými radami, k osobným údajom Vašich zákazníkov sa tak dostanú iba tí, ktorí to nutne potrebujú pre svoju prácu. Napríklad definíciou práv pomocou rolí pridelite prístupové práva jednotlivým pracovným pozíciám – iné budú mať účtovníčky, iné skladníci.

Na inštaláciu produktových radov pracujúcich s SQL technológiou potrebujete Microsoft SQL Server. Konkrétne systémové požiadavky na pracovné stanice jednotlivých užívateľov potom nájdete na www.stormware.sk/systemove-pozadavky/.

Odporúčame prejsť na produktové rady POHODA SQL alebo E1, ak...

...požadujete vysokú úroveň zabezpečenia dát.

...potrebujete k svojim dátam pristupovať vzdialene.

...chcete sami vytvárať užívateľské agendy bez použitia externej aplikácie.

...veľkosť Vašej najväčšej databázy (účtovnej jednotky) dosahuje 70 MB a viac.

...vzhľadom na svoje podnikateľské aktivity plánujete nárast objemu dát.

...využívate veľké množstvo účtovných jednotiek.



Čo to znamená SQL?

Pod skratkou SQL sa skrýva pojem Structured Query Language, čo by sme mohli preložiť ako štrukturovaný dotazovací jazyk. Ide o jednoduchý a zároveň robustný nástroj pre jednotnú úroveň prístupu k dátam v dátových úložiskách. SQL jazyk nie je závislý na ďalších vývojových a implementačných nástrojoch, neobsahuje totiž samostatné nástroje na tvorbu aplikácií.

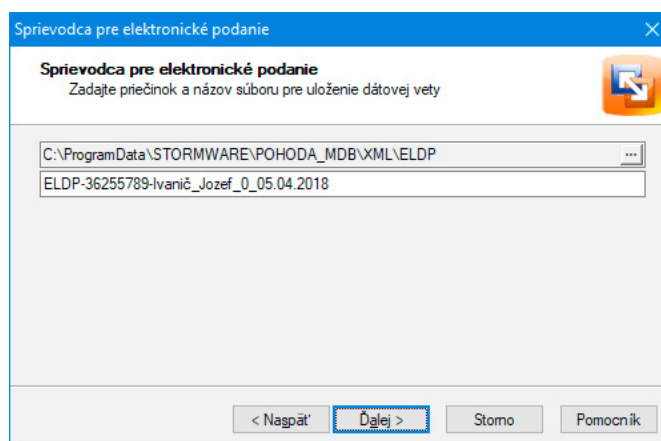
7.3. Prenos dát z/do programu POHODA

Keď máte vyriešené zabezpečenie dát v programe POHODA a nastavený prepracovaný systém prístupových práv, nezabudnite tiež na prenos údajov z/do programu POHODA. Dáta zo svojho ekonomického systému určite odosielate tretej strane (či už sú to faktúry zasielané zákazníkovi, alebo prehľady na sociálnu poisťovňu) alebo ich naopak od tretej strany prijímate a do programu následne importujete (napr. keď máte s programom POHODA prepojený e-shop alebo inú externú aplikáciu). Veľakrát ide o tie najcitlivejšie informácie – preto čím menej „sprostredkovateľov“ tým lepšie.

Oficiálne dokumenty ľahko odošlete do aplikácií finančnej správy, zdravotných poisťovní, či sociálnej poisťovne priamo z programu POHODA. Pomôže vám s tým sprievodca pre elektronické podanie, ktoré vyvoláte cez povel pod ponukou Záznam pri danom priznaní, prehľade, oznámení.

Pri bežnom odosielaní tlačových výstupov (napr. vydávaných objednávok e-mailom) ich aspoň zaheslujte – stačí upraviť nastavenie tlače (vo výklopnom menu PDF/Nastavenie PDF ... zadajte na záložku Zabezpečenie požadované heslo tlačovej zostavy).

TIP Využívate služby technickej podpory STORMWARE? Potom na bezpečný prenos databáz používajte servisnú schránku dostupnú na www.stormware.sk/zc/schranka.



8. GDPR v praxi

Implementácia nariadenia GDPR do praxe je pre mnohých podnikateľov nepredstaviteľná. Vybrali sme pre vás niekoľko príkladov zo života, vďaka ktorým si lepšie predstavíte spracovanie osobných údajov v spolupráci s programom POHODA.

Marketingová agentúra

Ako marketinová agentúra máte na svojich webových stránkach možnosť jednorázovej registrácie na odber newsletteru – e-booku s marketingovými tipmi. Registrácia má obmedzenú platnosť 3 mesiace, počas tejto doby užívateľom každý týždeň chodí časť e-booku. V programe POHODA si tak nadefinujete nový dôvod spracúvania osobných údajov, „Zasielanie reklamných oznámení“, na základe poskytnutého súhlasu s platnosťou 3 mesiace. Tento dôvod priradíte konkrétnym adresám na záložke GDPR.

Pred koncom súhlasu (napríklad po 2 mesiacoch od registrácie) si tieto adresy môžete jednoducho vyfiltrovať a zaslať im vlastnú ponuku profesionálnej marketingovej komunikácie. Potom, čo sa ju 100 užívateľov (z pôvodných 350 registrovaných) rozhodne využiť, priradíte im ďalší dôvod spracúvania údajov, tentokrát na základe zmluvného vzťahu. Medzitým si jeden z týchto užívateľov vyžiada doložiť údaje, aké o ňom spracováate. Na pár kliknutí si tak zobrazíte, aké údaje o ňom evidujete a na základe čoho – v tomto prípade rovno na základe dvoch dôvodov: zasielanie reklamných oznámení a zmluvného vzťahu.

SZČO – technik

Predávate, montujete a opravujete plynové kotle, tieto služby propagujete tiež na svojich webových stránkach. Pán Novák sa prihlásil na odber obchodných oznámení, ktoré obsahujú praktické informácie o revízii kotla. Do agendy Adresár programu POHODA tak nahráte údaje zadané pri registrácii (meno a e-mail) a na záložku GDPR tiež informácie o ich spracovaní na základe súhlasu so zasielaním obchodných oznámení.

Potom vás pán Novák telefonicky kontaktuje a chce vypracovať nezáväznú ponuku. Na tieto účely vám poskytne znova svoje meno a e-mail, ale tiež adresu s telefónom. Doplníte teda chýbajúce údaje k jeho záznamu do adresára a v agende Vydané ponuky vystavíte požadovanú ponuku na plynový kotol. Informácia o vystavenej ponuke sa prepíše tiež do agendy Adresár na záložku GDPR, a to ako vystavený predpredajný doklad. Stačí vybrať povel Aktualizovať dátumy použitia adresy ... z ponuky Záznam.

- Ak ponuku pán Novák nakoniec nevyužije, mali ste po vami stanovenej lehote jeho adresu a telefón v súlade s GDPR z adresára vymazať. (Meno a e-mail pána Nováka môžete tak či tak evidovať s neobmedzenou platnosťou, kým súhlas so zasielaním obchodných oznámení neodvolá.)
- Ak si kotol nakoniec kúpi, vystavíte mu v agende Vydané faktúry predajný doklad. Táto informácia sa potom objaví tiež v adresári na záložke GDPR vo forme dátumu vystavenia predajného dokladu.

Lehotu spracovania údajov pri predpredajných, predajných a popredajných dokladoch si môžete nastaviť v agende Globálne nastavenie.

Účtovníčka

Ako účtovníčka spracováate jednoduché účtovníctvo, príp. podvojné účtovníctvo 25 podnikateľom a firmám. Pretože účtovné dáta obsahujú veľké množstvo osobných údajov, ste zákonite ich sprostredkovateľom a vaši klienti sú ich prevádzkovatelia. Okrem ich evidencie v účtovnom programe máte potrebnú dokumentáciu (faktúry, dodacie listy apod.) zaradenú v šanónoch. Ako postupovať?

V prvom rade si ošetríte spracúvanie údajov a ich zabezpečenie zmluvne so všetkými 25 klientmi, kde bude okrem iného upravené ukladanie dát v účtovnom programe i v spomínaných šanónoch. Dôležitá bude tiež bezpečnosť prenosu dát klient-účtovníčka. Všetky výstupy z účtovného programu pre istotu zaistíte heslom – POHODA to umožňuje nastaviť priamo v priebehu exportu dokumentu v dialógovom okne Tlač.

Na záver je dôležité podotknúť, že iniciatíva by mala vychádzať od vašich klientov, pretože oni sú prevádzkovateľmi údajov.

E-shop

Vo svojom e-shope predávate ručne vyrobený tovar pre maminky s deťmi. Keďže údaje svojich zákazníkov evidujete pre účely plnenia zmluvy, t.j. na základe objednávky im zasielate tovar, nie je potrebné zaobštarávať súhlas na spracovanie osobných údajov. V programe POHODA tak jednoducho vystavíte faktúru a priamo k údajom zákazníka v adresári priradíte na záložku GDPR účel „Plnenie zmluvy“ a zadáte obdobie platnosti – počas tohto obdobia môžete evidovať zákazníkove osobné údaje. Druhou možnosťou je využiť dátumy predpredajných, predajných a popredajných dokladov, ktoré POHODA vypisuje na záložke GDPR po vystavení príslušného dokladu a zvolení povelu Aktualizovať dátumy použitia adresy ... z ponuky Záznam. Samostatný dôvod spracúvania tak už nie je potrebné na záložku písať. Akou cestou sa vydáte, je len na vás – z hľadiska GDPR je dôležité, aby dôvod pre spracúvanie údajov existoval.

Získavanie súhlasu vás čaká iba v prípade, že spravujete osobné údaje z iného ako zákonného dôvodu – napríklad zasielate zľavy a ponuky užívateľom registrovaným na odber vašich e-mailov. Tieto súhlasy je preto potrebné zrevidovať a upraviť podľa nariadenia GDPR. V programe POHODA potom vybraným kontaktom jednoducho priradíte dôvod – Súhlas („Zasielanie obchodných oznámení“).

9. Najčastejšie otázky a odpovede

? Plánuje POHODA rozšíriť svoje funkcie s ohľadom na nariadenie GDPR?

Áno, zameriava sa najmä na jednoduchšiu správu osobných údajov, ich vkladanie, triedenie a následné spracovanie. Primárne sa tieto rozšírenia budú týkať agendy Adresár. O novinkách v oblasti ochrany osobných údajov v programe POHODA zákazníkov budeme priebežne informovať štandardnými komunikačnými kanálmi (e-mailové spravodaje, časopis Moja POHODA, internetové stránky apod.).

? Čo by sme mali pripraviť, aby bolo všetko podľa nariadenie GDPR splnené? Ako je ekonomický systém POHODA pripravený na nariadenie GDPR?

Uvedenie organizácie do súladu s GDPR by malo primárne vychádzať z analýzy práce s osobnými údajmi, s ktorými pracujete, t.j. ich kategorizácia a typizácia, legitimita ich získania, minimalizácia ich vlastníctva z hľadiska účelu a času držania, ich zabezpečenie a pod. Následne by malo dôjsť k prijatiu vnútornej koncepcie, vykonaniu procesných zmien a k zavedeniu opatrení, ktoré zodpovedajú zásadám ochrany osobných údajov tak, ako nariadenie vyžaduje. K týmto činnostiam vám môže byť software nápomocný, avšak dokáže pokryť iba časť požiadaviek GDPR.

Náš produkt POHODA má už teraz integrované niektoré funkcionality smerujúce k naplneniu mnohých jednotlivých požiadaviek nariadenia GDPR, na ďalších rozšíreniach pracujeme. Zameriava sa najmä na jednoduchšiu správu osobných údajov, ich vkladanie, triedenie a následné spracovanie. Primárne sa tieto rozšírenia budú týkať agendy Adresár. O novinkách v oblasti ochrany osobných údajov zákazníkov priebežne informujeme, viď napr. novinky v produkte POHODA a článok na strane 14 časopisu Moja POHODA Január 2018 alebo článok na strane 18 časopisu Moja POHODA Október 2017. (Informácie uvedené v oboch vydaniach sa vzťahujú vždy k aktuálnym verziám programu.)

? Budeme si musieť kúpiť novú verziu programu POHODA s kompletou podporou GDPR, alebo potrebné aktualizácie poskytnete zadarmo?

Užívatelia aktuálnych verzií programu POHODA budú mať funkcionality súvisiace s nariadením ako súčasť aktualizácií. Špeciálne by ste si tak nič nepriplácali.

Samozrejme záleží tiež na vami použitom produktovom rade (<https://www.stormware.sk/pohoda/rady/>), pretože napr. POHODA E1 už teraz umožňuje evidovať históriu užívateľských úprav v agende Adresár, vytváranie voliteľných parametrov a pod. Prípadné nové funkcie súvisiace s GDPR, ktoré sa budú týkať práve možností, ktoré ponúka až rad POHODA E1, nebudú teda z princípu dostupné užívateľom nižších produktových radov programu POHODA.

? Poskytnete mi ako zákazníkovi spoločnosti STORMWARE nejaký dokument, že je ekonomický systém POHODA v súlade s GDPR?

Certifikácia slúži ako verejne dostupná garancia, najmä pre dotknuté osoby, že prevádzkovateľ resp. sprostredkovateľ bol preverený vo vzťahu k dodržiavaniu povinností podľa GDPR. Samotná certifikácia však neznižuje zodpovednosť prevádzkovateľa alebo sprostredkovateľa dodržiavať GDPR.

Certifikácia je proces vykonávaný vybranými subjektmi (tzv. certifikačnými subjektmi), ktorého účelom je preukázanie súladu spracovateľských operácií s GDPR. Certifikáciu majú vykonávať tzv. certifikačné subjekty, ktorými sú verejnoprávne alebo súkromnoprávne subjekty s primeranou úrovňou odborných znalostí vo vzťahu k ochrane osobných údajov, ktoré sú akreditované buď dozorným orgánom alebo národným akreditačným orgánom.

Certifikácia predstavuje možnosť (nie povinnosť) pre prevádzkovateľov a sprostredkovateľov preukázať, že vo vzťahu k daným spracovateľským operáciám dodržiavajú príslušné ustanovenia GDPR. Uvedené bude kontrolované zo strany nezávislých certifikačných subjektov.

V súčasnosti v SR ešte neexistujú akreditované certifikačné subjekty, ktoré by certifikáciu vykonávali. Akonáhle bude možné o certifikáciu zažiadať, pravdepodobne tak učiníme, akonáhle to bude možné, aby sme mohli doložiť súlad požiadaviek, ktoré GDPR na naše programy kladie.

Aktuálne teda pripravujeme materiály mapujúce spracovanie osobných údajov v rámci našich firemných procesov. Tie, ktoré budú určené dotknutým osobám, budeme postupne zverejňovať.

V tomto momente teda nie je možné doložiť oficiálnu certifikáciu súladu s GDPR s akýmkoľvek programom.

*Aktuálne k 1. 4. 2018

? Naša firma má zakúpenú licenciu programu POHODA od spoločnosti STORMWARE. Kto je z pohľadu GDPR prevádzkovateľ a kto sprostredkovateľ osobných údajov?

Spoločnosť STORMWARE bude vystupovať ako sprostredkovateľ v prípadoch, kedy jej budú zaslané zákaznicke dáta, resp. keď jej bude umožnené s vašimi údajmi alebo s údajmi vašich zákazníkov pracovať (napr. pri vzdialenej správe, školeniach s použitím týchto údajov a pod.). V takomto prípade ste prevádzkovateľom osobných údajov a so spoločnosťou STORMWARE bude potrebné uzatvoriť sprostredkovateľskú zmluvu.

V roli prevádzkovateľa bude STORMWARE vystupovať v iných prípadoch, napr. v súvislosti s e-mailovými

otázkami, zákazníckou podporou a v rámci obchodného vzťahu.

? V našej firme pracujeme s účtovným systémom POHODA. Kde nájdeme sprostredkovateľskú zmluvu?

Sprostredkovateľskú zmluvu do času účinnosti Nariadenia 2016/679 sprístupníme, našich zákazníkov o tom budeme informovať štandardnými komunikačnými kanálmi.

? Do adresára programu POHODA ukladáme i kontakty na zamestnancov zákazníkov/klientov (mailové adresy, mobilné kontakty), musíme, v súvislosti s GDPR, žiadať o súhlas zamestnancov zákazníka/klienta, uložiť si tieto kontakty?

V prípade spracúvania osobných údajov musí byť ošetrový právny základ ich spracúvania. Zamestnávateľ môže bez súhlasu zamestnanca jeho osobné údaje poskytnúť v rozsahu upravenom v § 78 ods. 3 zákona č. 18/2018 Z. z., ktorý hovorí: „Prevádzkovateľ, ktorý je zamestnávateľom dotknutej osoby, je oprávnený poskytovať jej osobné údaje alebo zverejniť jej osobné údaje v rozsahu titul, meno, priezvisko, pracovné zaradenie, služobné zaradenie, funkčné zaradenie, osobné číslo zamestnanca alebo zamestnanecké číslo zamestnanca, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, adresa elektronickej pošty na pracovisko a identifikačné údaje zamestnávateľa, ak je to potrebné v súvislosti s plnením pracovných povinností, služobných povinností alebo funkčných povinností dotknutej osoby. Poskytovanie osobných údajov alebo zverejnenie osobných údajov nesmie narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby.“

Od zamestnancov zákazníka/klienta súhlasy vyžadovať nie je potrebné vzhľadom na predmetné ustanovenie zákona č. 18/2018 z. z. Ide o vzťah prevádzkovateľa, ako užívateľa programu POHODA a jeho obchodného partnera. Je teda povinnosťou obchodného partnera napr. informovať svojich zamestnancov, že ich mailové adresy budú poskytnuté príjemcovi. Riešením by mohlo byť dať do obchodných zmlúv ustanovenie, kde by bolo upravené, že obchodný partner prehlasuje, že disponuje právnym základom na to, aby Vám poskytol osobné údaje svojho zamestnanca a kedykoľvek na žiadosť prijímateľa vie tento právny základ doložiť. Je však ale podľa nariadenia pravdou, že údaje o zamestnancoch vašich zákazníkov/klientov by mali byť aktuálne. T.j. v momente, kedy zamestnanec už nie je zamestnancom danej firmy, mal by Vám to váš zákazník/klient oznámiť, a aj toto odporúčame ošetriť v obchodnej zmluve.

? Ako bude program POHODA zabezpečovať šifrovanie údajov v databáze?

Podľa čl. 32 ods. 1 písm. b) nariadenia GDPR by malo byť postačujúce definovanie rolí, resp. prístupových práv v programe POHODA (napr. k jednotlivým agendám programu). Užívatelia však môžu využiť i ďalšie funkcie programu:

1. čiastočné zabezpečenie databázy – t.j. databáza bude zabezpečená interným heslom programu a bude tak chránená proti prístupu z iných programov.

2. úplné zabezpečenie – t.j. zvolená databáza bude zabezpečená interným heslom programu a zviazaná so systémovou databázou. Heslom, ktoré užívateľ zvolí, je chránený neoprávnený prevod databázy do inej inštalácie programu POHODA. Bez hesla potom nie je možné databázu previesť ani do inej inštalácie programu POHODA.

Ako ďalší stupeň ochrany údajov je prípadne možný prechod na vyšší rad programu, a to POHODA SQL alebo POHODA E1, kde je použitá technológia klient-server a databáza SQL poskytuje ešte vyšší stupeň ochrany údajov.

S ohľadom na samotné nariadenie GDPR a na vyššie uvedené dôvody sa údaje v databázach ekonomického systému POHODA nešifrujú. Pre úplnosť uvádzame i citáciu príslušnej časti nariadenia GDPR:

Článok 32 – Bezpečnosť spracúvania

1. Prevádzkovateľ a sprostredkovateľ prijímú so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku, pričom uvedené opatrenia prípadne zahŕňajú aj:

- a) pseudonymizáciu a šifrovanie osobných údajov;
- b) schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;
- c) schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu;
- d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

? Akým spôsobom je najvhodnejšie získať súhlas vo vzťahu k osobným údajom podľa zákona č. 122/2013 Z. z.? Stačí e-mailom?

Súhlas je potrebné predovšetkým preukázať. Musí byť teda zaznamenaný preukázateľne a musí byť v prípade potreby dokladovateľný, v tomto ohľade teda nie je problém ho mať e-mailom. Ďalej súhlas musí byť dobrovoľný, nie je možné ním podmieniť čerpanie nejakej služby. Musí byť tiež jednoznačný v účele a rozsahu, musí byť oddelený napríklad od obchodných podmienok, nesmie byť schovaný v zmluvách a pod. Tiež musí byť stanovené, za akým účelom je poskytnutý, napríklad za účelom zasielania obchodných informácií. V neposlednom rade musí byť súhlas informovaný, t.j. musí byť jasné, komu je súhlas udelený, že sa neodovzdáva mimo EU a ako je možné ho odvolať.

? Bude vhodné súhlas so spracúvaním osobných údajov premietnuť v obchodných podmienkach?

Pri súhlase je dôležitý jednoznačný prejav vôle dotknutej osoby (súhlas teda musí byť udelený jednoznačným prejavom vôle osoby). Z tohto prejavu musí byť zjavné, že osoba skutočne chcela udeliť súhlas so spracúvaním osobných údajov, nie že iba vyjadrovala súhlas s obchodnými podmienkami uzavretím zmluvy, poprípade že iba nevyjadrila nesúhlas. Preto by takýto súhlas nemal byť súčasťou všeobecných obchodných podmienok, mal by byť naopak oddelený.

? Osobným údajom je podľa GDPR aj evidencia dochádzky zamestnanca. V práci na chodbe máme dochádzkové hodiny a vedľa nich sú karty zamestnancov s evidenciou dochádzky v aktuálnom mesiaci, ako je možné toto ošetriť s prihliadnutím na GDPR?

Osobnými údajmi sú všetky informácie o fyzickej osobe (o subjekte údajov), ktoré je možné priamo či nepriamo identifikovať, najmä odkazom na určitý identifikátor. Je to napríklad meno, identifikačné číslo, lokalizačné údaje, sieťový identifikátor alebo jeden či viac zvláštnych prvkov fyzickej, fyziologickej, genetickej, psychickej, ekonomickej, kultúrnej alebo spoločenskej identity tejto fyzickej osoby. Z tohto pohľadu karty zamestnancov obsahujú osobné údaje a nariadenie GDPR sa na ich spracovanie vzťahuje, aj keď sa jedná o fyzické záznamy.

Dôvodom evidencie dochádzky je splnenie právnej povinnosti a je na spoločnosti, akým spôsobom zaistí ochranu týchto osobných údajov v súlade s nariadením GDPR. Je potrebné nastaviť primerané technické a organizačné opatrenia.

? Ako odporúčate riešiť marketingové e-maily, čo sa týka GDPR?

Je to trochu zložitejšia situácia, pretože marketingové e-maily môžeme rozdeliť do dvoch skupín:

- E-mailing, ktorý sa ako marketingový môže tváriť, ale obsahuje informácie napríklad o skutočnosti, že objednaná služba už končí, a vy len príjemcu informujete o službe novej či lepšej. To môže byť chápané ako oprávnený záujem prevádzkovateľa, kedy uplatníte legitímny titul – zmluvný vzťah a nepotrebujete teda žiadny ďalší súhlas subjektu.
- E-mailingové oznámenia, typicky obsahujúce nejaký produkt či službu nesúvisiace s už poskytovanou službou či dodaným produktom, postrádajú oprávnený záujem prevádzkovateľa. Preto je potrebné na takýto e-mailing mať už dopredu súhlas subjektu so zasielaním obchodných oznámení.

? Môže nám dať niekto súhlas so spracovaním osobných údajov cez telefón?

Podľa nariadenia GDPR, nemusí byť súhlas daný písomne, či elektronicky. Môže byť získaný rôznymi formami, ale musí byť zdokumentovaný, či už pre účely kontroly zo

strany úradov, ale i pre samotnú firmu/spoločnosť aby vedela, kto presne je ten, kto súhlas po telefóne udelil. V momente, keď sa rozhodne dotyčná osoba odvolať svoj súhlas, tak by mala mať možnosť súhlas odvolať rovnakou formou. Ak teda niekto súhlas udelí telefonicky, tak by ho telefonicky mal i vedieť odvolať. Pričom záznam o odvolaní musí byť tiež zabezpečený.

K telefonicky získaným súhlasom musí byť teda zabezpečená dostatočná archivácia, tzn. okrem iného aj uložený nahratý záznam, kde bol súhlas udelený.

? Bude v súlade s nariadením GDPR posielanie zaheslovaných výplatných pások e-mailom (priamo z programu POHODA)?

Podľa nariadenia GDPR by spoločnosť mala prijať primerané technické a organizačné opatrenia, ktoré bližšie, či podrobnejšie nariadenie nešpecifikuje.

Ak výplatné pásky, zasielané zamestnancom priamo z programu POHODA, budú zaheslované, tak i v prípade doručenia nesprávnemu príjemcovi výplatnú pásku nie je možné otvoriť. Je teda zabezpečené, že sa neoprávnená osoba k osobným údajom iného zamestnanca nedostane.