Magazín GDPR
číslo 1/2018

SOFTbit software

... Máme řešení i pro Vaši společnost

www.softbit.cz

Vážení zákazníci

Přinášíme Vám první číslo našeho nepravidelného magazínu věnovaného tématice ochrany osobních údajů podle GDPR. V následující době plánujeme zasílání i dalších magazínů vždy v okamžiku, kdy budeme mít pro Vás další nové zajímavé informace k této tématice. Věříme, že Vám informace, které získáte díky našemu magazínu, budou užitečné při lepším zajištění procesů v ochraně osobních údajů ve Vaší organizaci podle GDPR.

Naďa Lukášková
pracovník zákaznické podpory

Obsah

Stav nařízení GDPR v České legislativě k dubnu 2018	3
Co bychom měli všichni udělat v souvislosti se zavedením GDPR v naší organizaci	3
Nový modul GDPR v rámci informačního systému SQL Ekonom	5
SQL Ekonom a nové funkce k souladu s GDPR	7
Naše společnost jako zpracovatel podle nařízení GDPR?	7
Mzdy Soft PC a GDPR	8
Mzdy VEMA a GDPR	8
Základní pojmy GDPR ve stručnosti	12
Odpovědi na základní pojmy k problematice GDPR	15
GDPR v otázkách a odpovědích	16
Desatero zpracování pro správce	24
Zabezpečení odesílaných příloh elektronickou poštou – doplnění souboru heslem	25
Nabídka služeb GDPR	26

Stav nařízení GDPR v České legislativě k dubnu 2018

Jak jistě mnozí z Vás víte, vláda dne 21. 3. 2018 schválila návrh zákona o ochraně osobních údajů podle nařízení GDPR. Tento návrh využívá řadu výjimek, které mu nařízení o ochraně osobních údajů umožňuje. V následujících řádcích uvádíme některé z těchto výjimek.

- Posunutí hranice dítěte na 15 let z 16 let dle nařízení EU
- Snížení sankcí pro organizace státní správy nebo dokonce jejich prominutí
- Zmenšení počtu subjektů s povinným zřízením pozice „Pověřence pro ochranu osobních údajů“ – jedná se například o knihy apod.

Jak je patrno z pozměňovacích návrhů, neočekávejme zásadní změny proti původnímu nařízení GDPR, které musí všechny členské státy Evropské Unie přijmout do své legislativy.

V této době není vůbec jasné, kdy bude a s jakými změnami nový zákon přijat a projde celým legislativním procesem. Odhadujeme, že se tak stane až v průběhu letních měsíců či na podzim.

Přestože se česká lokalizace nařízení GDPR v podobě nového zákona nestihne do 25. 5. 2018 (od tohoto dne má nové nařízení být uvedeno v platnost), pravidla daná novým nařízením Evropského parlamentu ze dne 27. 4. 2016 budu platná i v České republice v plném rozsahu.

Tímto okamžikem bude zároveň zrušen Zákon 101/2000 Sb. o ochraně osobních údajů.
Jakmile budeme znát nové důležité informace, budeme Vás o nich informovat.

Co bychom měli všichni udělat v souvislosti se zavedením GDPR v naší organizaci

V tomto článku Vás seznámíme formou jednoduchých bodů se základy přípravy všech činnosti a mechanismů ve Vaší organizaci, které zajistí soulad s GDPR.

Povinnosti správce (společnosti/organizace) – na co bych neměl zapomenout

- Zajistím zpracování vnitřního auditu k ochraně osobních údajů
- Pojmenuji veškeré činnosti, kde osobní údaje zpracovávám a přiřadím si k těmto činnostem právní nárok
- Stanovím, k jakému účelu osobní údaje v jednotlivých činnostech zpracovávám
- Pokud nemám právní nárok k zamýšlenému účelu osobní údaje zpracovávat, vyžádám si od fyzických osob souhlas
- Podle právního nároku stanovím dobu, po kterou mohu tyto informace zpracovávat a definuji způsoby anonymizace
- Vytipuji si všechny osobní údaje, které zpracovávám zbytečně a tyto bez zbytečného odkladu anonymizuji
- Udělám si inventarizaci všech dokumentů a elektronických dat, která eviduji, zda některé nezpracovávám po době jejich právního nároku, a tyto skartuji, smažu atd.
- Zkontroluji aktuálnost informačních systémů na soulad s GDPR
- Pokud provozuji e-shop, zkontroluji jeho aktuálnost v souladu s GDPR
- Zkontroluji a aktualizuji veškeré smlouvy se zpracovateli osobních dat

- Stanovím pracovníka, který v organizaci bude mít na starost kontrolu souladu s nařízením GDPR
- V mém zájmu stanovím pracovníka nebo externí společnost pro služby „Pověřence pro ochranu osobních dat“ (u organizací, které mají povinnosti to je automatické)
- Zpracuji srozumitelnou vnitropodnikovou směrnici k ochraně osobních údajů
- Vytvořím v organizaci mechanismy pro správnou ochranu osobních údajů, které budou popsány ve výše uvedené směrnici
- Proškolím zaměstnance se zásadami GDPR podle sestavené směrnice
- Dbám na plnění zabezpečení osobních dat v souladu s GDPR všemi pracovníky společnosti

Povinnosti zaměstnance – co mám dělat?

- Ukládám elektronické dokumenty jen na datová uložiště v organizaci k tomu určená
- Udržuji uživatelská hesla do počítačů a informačních systémů v tajnosti, nikde si je nezaznamenávám ani nesděluji ostatním pracovníkům
- Nesděluji informace s osobními daty osobám, které nemají k těmto informacím oprávnění je zpracovávat
- Posílám emaily s osobními daty pouze na ověřené adresy
- Emaily s osobními daty většího rozsahu nebo citlivými posílám pouze formou zaheslované nebo zašifrované přílohy
- Se státní správou komunikuji přes zabezpečené rozhraní služby Datové schránky České pošty
- Listinné dokumenty obsahující osobní data zabezpečuji tak, aby se k nim nemohla dostat neoprávněná osoba
- Uzavírám si v době nepřítomnosti dokumenty s osobními daty do skříní k tomu určených
- Při odchodu od počítače vždy uzamykám obrazovku PC (Windows-L)
- Bez vědomí vedení organizace nezasílám nevyžádaná obchodní sdělení zákazníkům bez jejich uděleného souhlasu
- Bez vědomí vedení organizace netelefonuji s obchodními nabídkami zákazníkům bez jejich uděleného souhlasu
- Elektronické a listinné dokumenty, které si vytvářím pro svoji potřebu, po ukončení jejich použitelnosti smažu či jiným způsobem likviduji (skartuji atd.)
- Znám práva fyzických osob a umím na jejich požadavky správně reagovat
- Neprovádím zálohy dat na externí zařízení, která nejsou k tomu určena, bez vědomí správce IT
- Neoslovováni zákazníky, dodavatele a jiné fyzické osoby za účelem cíleného marketingu bez platného souhlasu dané osoby
- Neukládám heslo pro automatické přihlašování do aplikací
- Nenavštěvuji na pracovišti webové adresy pro svoji soukromou potřebu
- Ke služební komunikaci s obchodními partnery používám výhradně služební email
- Naopak přes soukromý email nikdy nevyřizuji služební poštu
- Svůj služební telefon mám zajištěn přístupovým pinem či jiným zabezpečením proti zneužití při jeho zcizení
- Chráním přenosné notebooky a jiná zařízení, která využívám pro svoji práci proti zcizení či zneužití

Povinnosti správce IT – co bych měl mít na starost

- Pravidelně provádím zálohy elektronických dat na externí datové uložiště a tyto zálohy kontroluji
- Formou osvěty bráním nesystémovému provádění záloh zaměstnanci na jiná než k tomu určená zařízení
- Zabezpečuji datová uložiště proti neoprávněnému přístupu od zaměstnanců v organizaci nebo přes vnější přístup
- Nastavuji a kontroluji správnou sílu hesel zaměstnanců do informačních systémů i počítačů
- Nastavuji a kontroluji práva zaměstnanců tak, aby měli přístup pouze tam, kde mají oprávnění přistupovat (jak ve složkách, tak i v informačních systémech)
- Při ukončení pracovního poměru některého ze zaměstnanců jeho práva v datové síti ukončuji a zajištuji bezpečné uložení všech dokumentů a souborů pro další zpracování novým pracovníkem
- Kontroluji a hlídám správné nastavení, aktualizace a funkčnost antivirového programu na datovém serveru i stanicích
- Kontroluji a hlídám správné nastavení vstupní brány Firewall na datovém serveru
- Spravuji uživatelské účty a přístupy na datový server z internetu a dbám na maximální zajištění těchto přístupů
- V případě používaní přenosných počítačů (notebooků) zaměstnanci zajišťuji jejich ochranu a správné používání zaměstnanci (ideálně nastavuji šifrování datových disků)
- Likviduji správným způsobem již nepoužitelnou výpočetní techniku, zejména se zaměřuji na datové disky obsahující osobní i jiná důležitá data

Výčet jednotlivých povinností berte jako vodítko při zpracování vnitropodnikových procesů k ochraně osobních údajů ve Vaší organizaci. Seznam nemusí být úplný a může se měnit podle povahy, velikosti i zaměření Vaší organizace.

V případě, že budete chtít se zavedením jednotlivých procesů v souvislosti s ochranou osobních údajů podle GDPR, neváhejte nás ihned kontaktovat.

Nový modul GDPR v rámci informačního systému SQL Ekonom

Pro všechny naše zákazníky jsme připravili zcela nový modul GDPR v rámci informačního systému SQL Ekonom. Modul vychází vstříc všem zákazníkům, kteří budou potřebovat jednoduše a přehledně evidovat požadavky a práva fyzických osob (subjektu údajů).

Všechny fyzické osoby z řad zaměstnanců, zákazníků, dodavatelů, klientů organizací budou mít od 25. 5. 2018 řadu nových práv. Každá organizace musí o těchto požadavcích vést přehlednou evidenci, kterou doloží případné kontrole soulad s GDPR.

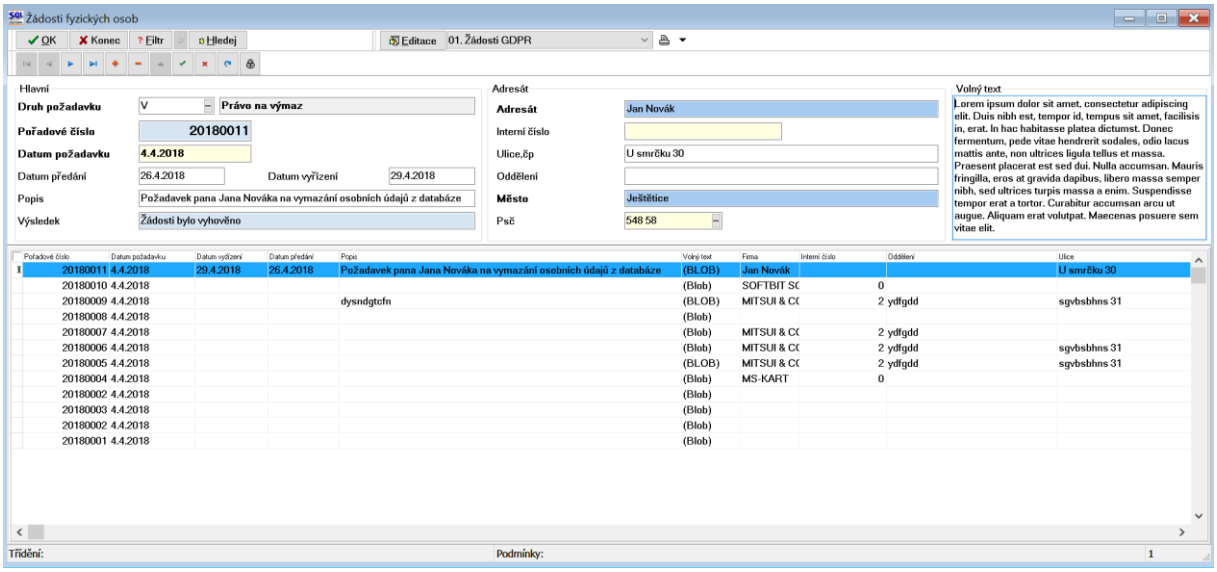
Jedná se hlavně o tato práva:

- Práva na přístup k osobním údajům
- Právo na výmaz (být zapomenut)
- Právo vznést námitku
- Právo na omezení zpracování
- Právo na přenositelnost údajů
- Právo na omezení automatického rozhodování

Dále každá organizace, která zpracovává osobní údaje na základě souhlasu, bude muset vést evidenci těchto souhlasů s datem od kdy, do kdy a k jakému účelu je souhlas platný.

Nový modul umí:

- Evidovat požadavky fyzických osob v rozsahu nových práv
- Evidovat souhlasy ke zpracování osobních údajů podle jednotlivých účelů
- Uchovávat veškerou dokumentaci k právům fyzických osob a jejich souhlasům
- Sledovat, zda požadavky jsou řešeny v zákonem stanovené lhůtě
- Zobrazovat podklady pro kontrolní orgán
- a další



Obrázek: Formulář žádostí o práva fyzických osob

Cenu nového modulu jsme stanovili podle součtu počtu fyzických osob, které každá společnost zpracovává, tj. počet zaměstnanců, počet dodavatelů a odběratelů z řad fyzických osob, počet klientů, dětí atd.

Ceník, uživatelé IS SQL Ekonom:

	Do 500 FO	Do 1000 FO	Do 3000 FO	Do 5000
Cena do 25.5.2018	1000,- Kč	2000,- Kč	3000,- Kč	4000,- Kč
Cena po 25.5.2018	1600,- Kč	3000,- Kč	4600,- Kč	5600,- Kč

Ceník, zákazníci, kteří nevlastní IS SQL Ekonom

	Do 500 FO	Do 1000 FO	Do 3000 FO	Do 5000
Cena do 25.5.2018	1700,- Kč	2700,- Kč	3700,- Kč	4700,- Kč
Cena po 25.5.2018	2300,- Kč	3700,- Kč	5300,- Kč	6300,- Kč

Modul si můžeme objednat přímo formou zaslání emailové objednávky na email softbit@softbit.cz. Při objednávce sdělte, prosíme, do počtu fyzických osob, které Vaše organizace spravuje a dále zda jste uživateli IS SQL Ekonom či ne.

Na základě objednávky Vám vystavíme licenční smlouvu a dodáme software pro evidenci požadavků a práv fyzických osob podle GDPR.

SQL Ekonom a nové funkce k souladu s GDPR

Informační systém SQL Ekonom obsahuje od verze 18.1.0 nové funkce, které zajišťují soulad s nařízením GDPR.

Jsou to hlavně tyto funkce:

- automatizovaná anonymizace osobních údajů fyzických osob po době právního nároku
- nastavení síly hesla a jeho platnosti pro všechny uživatele informačního systému
- podrobné nastavení přístupových práv do modulů SQL Ekonom s dělením na plné zpracování, prohlížení atd.
- sledování provedených operací jednotlivých uživatelů se zpětným výpisem
- výpis osobních údajů fyzické osobě
- sledování exportů dat ze systému s možností nastavení jejich omezení
- uložení veškerých dat v SQL databázi s vysokým zabezpečením proti neoprávněnému přístupu

V průběhu měsíce května Vám budeme posílat znovu manuál k nastavení jednotlivých funkcí tak, aby si každý uživatel mohl jednoduše nastavit zabezpečení osobních dat v souladu s GDPR.

V průběhu měsíce května budeme rovněž zasílat všem uživatelům informačního systému SQL Ekonom certifikát souladu s GDPR pro doložení do vnitřních směrnic k ochraně osobních údajů.

Naše společnost jako zpracovatel podle nařízení GDPR?

V poslední době se objevila řada informací o tom, že dodavatelé informačních systémů by měli být zároveň vůči správcům (uživatelům informačních systémů) podle nařízení GDPR v pozici zpracovatelů.

Tuto informaci rozšiřuje zejména Ministerstvo vnitra. Náš postoj k této informaci je v tuto chvíli tento. Vnímáme jako důležité pro každého našeho zákazníka informačních systémů, aby měl zajištěnu ochranu svých dat, ke kterým při provádění servisu máme přístup.

Kodex chování pracovníků naší společnosti obsahuje mimo jiné i nesdělování jakýchkoliv informací o společnosti zákazníka třetím osobám a veškeré takto získané informace pracovník používá pouze pro zajištění kvalitního servisu k dodanému software.

Z tohoto důvodu nabízíme všem našim zákazníkům možnost uzavření dodatku k licenční smlouvě obsahujícího zajištění mlčenlivosti o všech informacích, ke kterým mají naši pracovníci při zajištění servisu k dodanému software přístup.

Bude-li Vaše společnost chtít uzavřít s námi tento dodatek, prosím, kontaktujte centrálu naší společnosti. Znění dodatku Vám zašleme na požádání a v případě, že s tímto dodatkem budete souhlasit, můžeme jej bez odkladu uzavřít.

Podle nařízení GDPR však zajištění servisu k používanému software v případě, že se jedná o nepravidelnou službu související s opravou software, instalací nových verzí, opravou pořízených dat, školení obsluhy atd. není.

Zpracovatelem však může být například softwarová společnost, která zajišťuje pro zákazníka služby provádění záloh dat k dodanému software na svůj datový server nebo zajišťuje provádění měsíčních účetních uzávěrek apod.

Mzdy Soft PC a GDPR

Podobně jako informační systém SQL Ekonom, tak i mzdový systém Win Mzdy Soft PC dozná některých změn, které jej uvedou do souladu s GDPR.

V nové verzi mezd, která bude uvolněna v nejbližší době, bude v souvislosti s GDPR nová funkce týkající se výpisu osobních údajů fyzické osoby.

Na závěr uvádíme, že společnost Soft PC, která je autorem mzdového systému, již zavádí u zákazníků nový systém SQL mzdy Soft PC, který obsahuje řadu nový funkcí i v případě zajištění ochrany osobních údajů fyzických osob. O tomto novém programu Vás budeme informovat v našem květnovém magazínu.

Mzdy VEMA a GDPR

Tajemný modul GDPR, který vlastně neexistuje

Datum 25. 5. 2018, tj. počátek účinnosti Obecného nařízení na ochranu osobních údajů (GDPR), se nezadržitelně blíží. Proto pro vás společnost Vema a.s. připravila novým modul Vema GDPR, který byl vytvořen pro podporu splnění požadavků a povinností plynoucích z Nařízení GDPR v prostředí mzdových a personálních systémů Vema. Nasazení modulu, jeho nastavení a provoz bude vysvětleno na odborných seminářích.

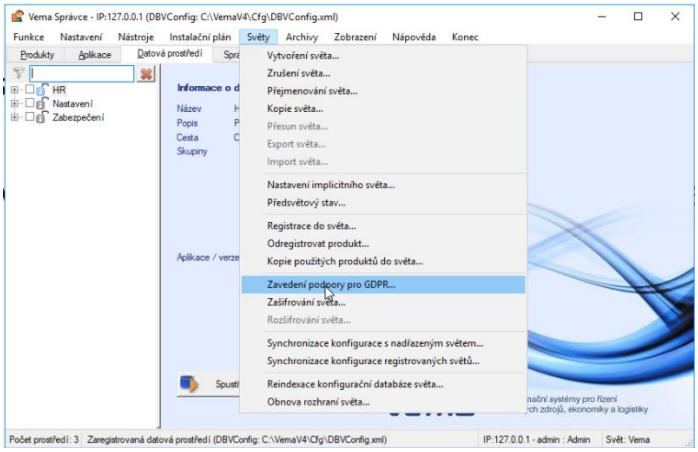
Takovýto seminář pro Vás připravujeme i v Rychnově n. Kn. Jeho termín bude zveřejněn v nejbližších dnech. Pro realizaci semináře by nám pomohla informace, zda o své účasti uvažujete. Pokud ano, prosím pošlete nám tuto informaci na email vema@softbit.cz, případně volejte na telefonní číslo 494 532 202. Stejnou cestou si můžete vyžádat i cenu modulu GDPR.

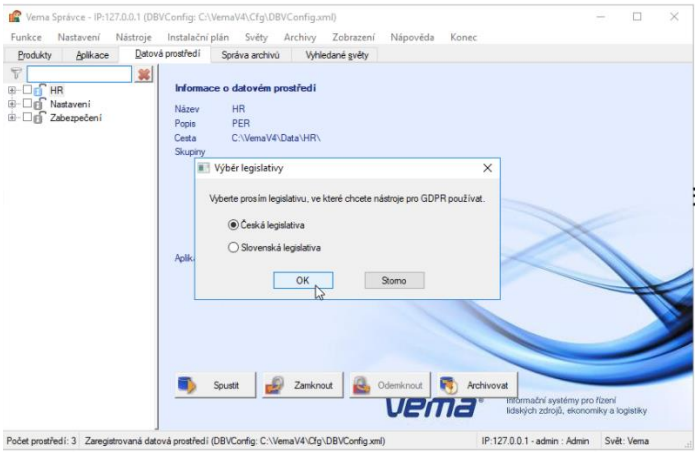
Každý zákazník, který si modul Vema GDPR již objednal, případně o jeho nákupu vážně uvažuje, by se měl tohoto odborného semináře rozhodně zúčastnit. Očekáváme, že prostá účast na semináři postačí k načerpání znalostí nutných pro zprovoznění modulu Vema GDPR svépomocí, stejně tak pro jeho každodenní používání. V případě potřeby jsme připraveni Vám s modulem GDPR pomoci.

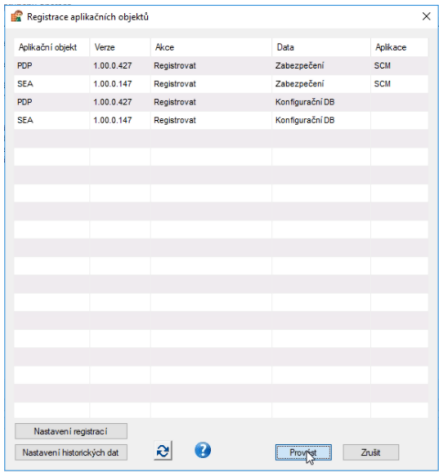
Nový modul s názvem GDPR, který společnost Vema vyvinula z důvodu změn v legislativě, vlastně modulem není.

Jedná se o licenci na sadu produktů. Tyto produkty nevyřeší problematiku GDPR u zákazníka, ale jedná se o silný nástroj, který výrazně usnadní implementaci GDPR. Konkrétně jde o produkty PDP a SEA.

Instalace a zavedení modulu GDPR je zajištěno podporou ve Správci a je velmi jednoduché.

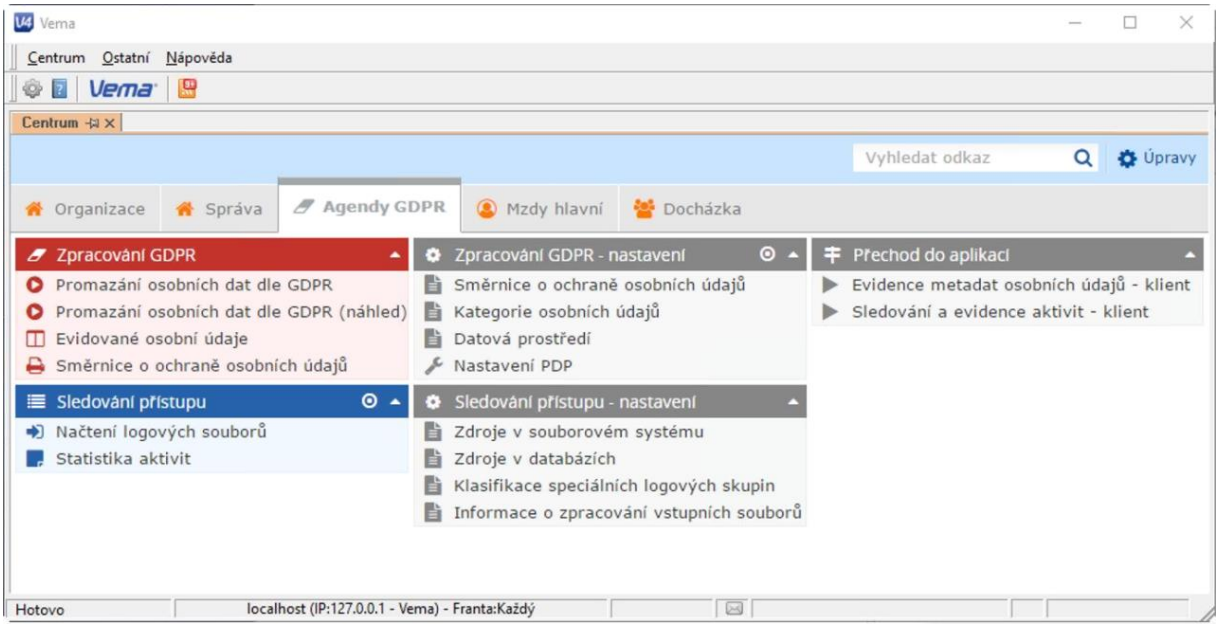






V čem Vám modul GDPR může pomoci? (funkcionality produktu PDP)

- podpora tvorby a tisku interních směrnic na ochranu osobních údajů
- Postupné mazání osobních údajů ve vazbě na konec platnosti právního důvodu pro jejich uchovávání
- Právo na informovanost subjektu údajů o evidovaných osobních údajích
- Právo subjektu údajů na přenositelnost osobních údajů
- Ochrana dat, šifrování, logování



Podpora tvorby a tisku interních směrnic na ochranu osobních údajů

Do Vema Centra přibude nový odkaz, který slouží jak pro editaci směrnice, tak pro tisk.
Jedná se o „polotovar“, každá organizace má jiná vnitřní pravidla a postupy.
Přílohou směrnice by měl být seznam tabulek s osobními údaji

Postupné mazání osobních údajů ve vazbě na konec platnosti právního důvodu pro jejich uchovávání

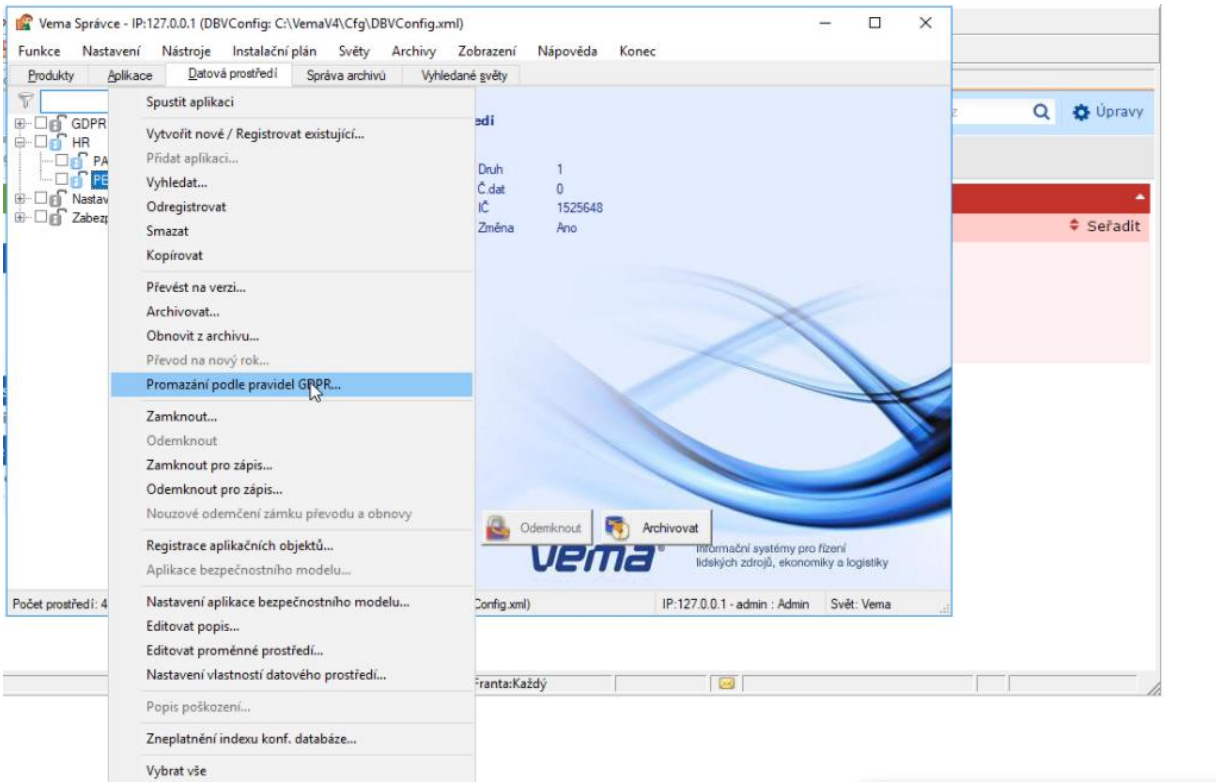
Základem správného fungování této funkce, je její správné nastavení.

- Nastavují se datová prostředí, ve kterých k mazání dochází.
- Nastavují se kategorie osobních dat
- Definuje se seznam tabulek s osobními daty
- Definuje se seznam položek s osobními daty v tabulkách

Samotné promazání osobních dat se spouští ručně, buď odkazem z Centra pro všechna registrovaná datová prostředí. Druhou možností je spuštění funkce ze Správce nad konkrétním datovým prostředím, případně jenom jedním subsystémem, např. PAM.

Funkce má limity:

- Podporují ji pouze aktuální verze aplikací, to znamená, že podpora ve starších verzích není technicky možná
- Nepromazávají se archivy, ale po obnově dat z archivu se funkce promazání dat nabídne podle aktuálně nastavených pravidel



Právo na informovanost subjektu údajů o evidovaných osobních údajích

V modulu GDPR je to ošetřeno dynamickým dokumentem se seznam tabulek a jejich hodnot, ve kterých jsou osobní data zadaného zaměstnance.

Právo subjektu údajů na přenositelnost osobních údajů

Údaje z dynamického dokumentu je možné exportovat do formátu XML, tím je splněna podmínka na strojově čitelný formát a také přenositelnost takovýchto údajů.

Ochrana dat, šifrování, logování

Samotné GDPR šifrování dat nevynucuje, v modulu GDPR se jedná o volbu.
V případě, že se zákazník rozhodne šifrování použít je to zajištěno šifrováním v rámci prostředků operačního systému. Šifruje se adresář se světem Vema.
Doporučuje se používat jen na vyhrazených serverových stanicích.

Funkcionality produktu SEA (sledování a evidence aktivit)

- Koncentrátor logů
- Načítá ze všech logů vybrané typy změn
- Dovoluje zobrazení přístupu jednotlivých uživatelů a rolí k osobním údajům
- Zobrazení aktivity uživatele v datech
- Načítání logů

Základní pojmy GDPR ve stručnosti

Ještě před startem platnosti nového nařízení GDPR o ochraně osobních údajů od 25. 5. 2018 Vás v následujícím článku chceme seznámit se základními pojmy, které by každý pracovník, který zpracovává osobní údaje, měl znát.

1. Důvod

Abychom mohli o nějaké kategorii lidí, například našich zákazníků nebo zaměstnanců, získávat a používat jejich údaje, musíme k tomu mít nějaký (právní) důvod. Velmi často jím bývají smlouvy, které s nimi uzavíráme. Pracovní smlouvy se zaměstnanci, kupní smlouvy nebo jiné se zákazníky.

Takovým důvodem je samozřejmě také zákon, který to ukládá, např. při vedení evidencí občanů státními orgány, ale i při vedení účetní a mzdové evidence v soukromé firmě. V některých případech může být důvodem ochrana našich práv, např. hlídá-li kamera náš cenný majetek před zlodějem nebo vandalem. Jindy to může být veřejný zájem na informacích o určitých osobách, zejména veřejně známých nebo veřejně činných.

Takové informace a jejich používání ale nemohou nepřiměřeně zasahovat do jejich soukromého života. Nenajdeme-li žádný z těchto důvodů, a přece bychom chtěli údaje o lidech získávat, např. o tom, jakému našemu zboží budou dávat přednost, je třeba je požádat, zda s vedením takových údajů budou souhlasit. Musíme ale mít na paměti, že souhlas je dobrovolný, nemůže jím být podmiňováno uzavření smlouvy, a když ho zákazník odvolá, má právo, aby byly takové údaje vymazány.

Když už si zákazník od nás něco koupil nebo objednal, nemusíme získávat jeho souhlas k zaslání další nabídky našeho zboží nebo služeb, nejčastěji zasílané na jeho e-mail. Jakmile však odpoví, že o takové obchodní sdělení nestojí, je nutné zasílání nabídek na jeho adresu ukončit. Není-li dán jiný důvod ke zveřejňování v databázi uchovávaných osobních údajů, např. kontaktních údajů zaměstnance do zaměstnání pro kontakt se zákazníky, je ke zveřejňování osobních údajů také třeba získat souhlas. Zvláštní důvody je třeba mít k tomu, abychom mohli získávat a používat kategorie údajů, které by mohly být zneužívány k diskriminaci lidí, např. údaje o zdravotním stavu.

2. Zásady

Vždy bychom si měli nejprve uvědomit, proč údaje o nějakých lidech potřebujeme nebo chceme získávat. Z toho je pak třeba vyjít při požadavku na poskytnutí údajů, abychom zbytečně o těch lidech nezaznamenávali informace, které vlastně vůbec nepotřebujeme. Rozsah údajů by tak měl být jen minimální, abychom dosáhli toho, co jsme si stanovili. Měli bychom dbát na to, aby získávané údaje byly přesné a jejich přesnost ověřovat. Možnost ověřit přesnost údajů z občanského průkazu dotyčné osoby není vyloučena, kopírování občanského průkazu i pasu je však až na zákonem stanovené výjimky nepřípustné.

Zaznamenané údaje nemohou být využívány v rozporu s původním cílem. Například na záznamu kamery je uložena spousta obrazových informací o všech osobách, které do sledovaného prostoru vstoupily. Jsou po přiměřenou dobu uchovávány, aby případně bylo možné policii doložit informace o pachateli trestného činu. Nemohou být, ale využívány k nedůvodnému sledování sousedů, třeba jen proto, že si někdo neočistil boty, nebo k nepřiměřenému kontrolování zaměstnanců na pracovišti.

Další zásadou je mít údaje jen tak dlouho, jak je potřeba. Ta doba se může v různých případech hodně odlišovat. Od několika dnů záznamu kamery, kdy je zřejmé, že se v té době nic mimořádného nestalo, až po desítky let u zákonem stanoveného uchovávání některých dokumentů, třeba mzdových listů. Ne vždy končí doba nutná k uchovávání všech údajů ukončením nějaké činnosti, např. ukončením pracovního poměru nebo naplněním smluvního ujednání. V úvahu je třeba brát jak lhůty stanovené zákonem pro uchovávání některých dokumentů, tak případné promlčecí lhůty pro možnost podání soudní žaloby a v případě listinných dokumentů i lhůty skartační.

3. Informace
Nejvíce nedorozumění a stížností vzniká z toho, že lidé nedostanou dostatečnou informaci o tom, proč své osobní údaje poskytují a co se s těmito údaji bude dále dít, komu budou případně předány. Již při získávání údajů je proto třeba dotyčnému člověku takové informace poskytnout, nejlépe v písemné podobě, ať již v místě, kde k získání údajů dochází nebo i prostřednictvím webových stránek.

Vyhovět je třeba i dalším právům, která mohou lidé uplatnit, jestliže jejich osobní údaje uchováváte a používáte. Právo na poskytnutí informací o svých údajích mají nejen ve chvíli jejich poskytnutí, ale mohou se dotázat i kdykoliv později. Pokud se to nedotkne práv jiných osob, má každý právo i na poskytnutí kopie svých údajů. Za další kopii už ale můžete požadovat přiměřený poplatek. K dalším právům patří i právo na opravu nepřesných údajů, právo vznést námitku, např. proti dalšímu zasílání marketingových nabídek, a také právo na výmaz údajů, ale pouze pokud není jiný důvod pro jejich další uchovávání.

4. Zabezpečení
Pokud máte údaje lidí jen na listinných dokumentech, a ne v počítači, vztahuje se na ně ochrana jen v případě, že jsou vedeny formou evidence fyzických osob.

Je třeba, aby listinné dokumenty, pokud se s nimi nepracuje, byly uchovávány v uzamčené zásuvce stolu nebo v uzamčené skříni a nebyly ponechávány v neuzamčené místnosti, pokud z ní odchází ten, kdo s nimi má pracovat. K údajům uloženým v počítači nebo jiném elektronickém zařízení může mít na základě správně zvoleného hesla přístup vždy jen ten, kdo je pověřen, aby s určitými údaji pracoval. U větších a složitějších systémů je také třeba pořizovat elektronické záznamy, které umožňují určit a ověřit, kdy, kdo a z jakého důvodu údaje používá, tzv. logy.

Pravidla bezpečnosti je třeba zachovávat i u elektronických prostředků používaných při různých cestách, např. je neponechávat bez dozoru v automobilu. Osobní údaje musejí být odpovídajícím způsobem zabezpečeny i při jejich přenosu elektronickými prostředky. Šifrování není povinné, je ho však třeba doporučit při zaslání většího objemu dat, zvláště pak citlivých, nejčastěji jde o zdravotní údaje pacientů. Jinak je vhodné volit formu zabezpečeného e-mailu (HTTPS). Neznamená to však, že prostý e-mail (HTTP) by nebylo možné nikdy použít, např. pokud jde jenom o jednoduchou domluvu se zákazníkem.

Pokud osobní údaje, např. svých zákazníků nebo zaměstnanců, předáte někomu jinému, aby s těmito údaji pracoval pro vás a místo vás, musíte s ním uzavřít smlouvu, ve které se zaváže, že bude údaje chránit stejně jako vy. Bez takové smlouvy byste pro předání údajů jiným osobám mimo firmu nebo organizaci museli získat souhlas dotčeného člověka, pokud nejde o

požadavek policie nebo jiného státního orgánu, který má právo si údaje potřebné pro svoji činnost vyžádat a je povinnost mu je poskytnout.

5. Co nového k tomu od 25. května 2018 přidává obecné nařízení o ochraně osobních údajů (GDPR)?
Pro menší firmu, která vede jen evidenci smluv se svými zákazníky a evidenci zaměstnanců, toho není zas až tak mnoho.

Záznamy o činnostech – všichni
Bude třeba vést záznamy o činnostech, které se s osobními údaji provádějí. Lze doporučit připravit si na to formulář s kolonkami a do nich zapsat informace požadované v článku 30 GDPR (záznam o evidenci smluv, o evidenci zaměstnanců, případně o slevovém programu pro zákazníky aj.). Takový zápis by pak neměl trvat déle než 10–15 minut.

Ohlašování případů porušení zabezpečení – všichni
Druhou obecně platnou povinností je ohlašování případů porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů podle článku 33 GDPR (do 72 hodin od zjištění takového incidentu). Hlásit je třeba závažné incidenty s předpokládanými závažnými důsledky, ne když se z papírově vedené evidence omylem založí jeden papír do jiného šuplíku, kde se za hodinu najde. Pokud dojde k úniku dat, např. v bance, kde máte uloženy peníze, a hrozilo by, že o ně můžete v důsledku toho přijít, bude mít banka povinnost oznámit to i vám, v krajním případě i veřejným oznámením takového závažného incidentu.

Kodexy a osvědčení – dobrovolně
Pokud v některých odvětvích, např. při podnikání, dochází ke stejným nebo velmi podobným činnostem s osobními údaji, může pro to být, např. profesním sdružením, vypracován kodex chování. Přihlášení se k takovému kodexu dokládá snahu být v souladu s obecným nařízením, není však povinné, stejně jako osvědčení o ochraně osobních údajů, o které bude možné požádat, ale povinné rovněž nebude.

Pověřenec pro ochranu osobních údajů – jen někdo
Úřady a jiné orgány, které rozhodují o právech občanů, a patří k nim i školy, budou muset jmenovat pověřence pro ochranu osobních údajů, osobu, která se bude této problematice věnovat a upozorňovat na případné nedostatky. Předpokládá se, že bude problematice ochrany osobních údajů v příslušném odvětví rozumět. Pověřencem může být jak vlastní zaměstnanec, tak externista. Poměrně široce tak lze využít možnosti, že jeden pověřenec bude moci takovou činnost vykonávat pro více úřadů, škol, ale i nemocnic, protože ty také budou mít povinnost pověřence jmenovat z hlediska velkého množství údajů o zdravotním stavu pacientů v informačním systému nemocnice. Pověřencem ale nemůže být šéf organizace nebo oddělení informatiky, protože by byl ve střetu zájmů.

Posouzení vlivu a konzultace s Úřadem – jen někdo
Stejně jako jmenování pověřence není ani posouzení vlivu na ochranu osobních údajů a předchozí konzultace s Úřadem pro ochranu osobních údajů povinností obecně platnou, týká se těch, kdo hodlají provádět s osobními údaji rozsáhlé rizikové operace, spočívající například v rozsáhlém profilování lidí prostřednictvím internetu, při kterém jsou pro marketingové účely získávány podrobné informace o jejich soukromém životě, nebo rizikovost spočívá ve využití nových technologií používaných, např. na velké množství údajů o zdravotním stavu pacientů. Seznam těchto operací bude Úřadem pro ochranu osobních údajů zveřejněn.

Sankce – vždy přiměřené
Flagrantního porušení obecným nařízením stanovených povinností při takových rizikových operacích prováděných ve velkém objemu dat, zpravidla velkými nadnárodními společnosti, se mohou týkat maximální, obecným nařízením stanovené sankce, dosahující značných částek. Strašit takovými sankcemi menší firmu nebo školu je nesmysl, stejně jako vydávání horentních částek, podstatně převyšujících výši pokut Úřadem pro ochranu osobních údajů ukládaných, za externí audity soulad s nařízením nezaručujícími. Případné sankce za porušení povinností obecného nařízení budou jako dosud přiměřené a v žádném případě nemohou být likvidační.

Odpovědi na základní pojmy k problematice GDPR

Protože přes pokročilé datum ještě někteří z Vás mají pouze omezené informace o novém nařízení GDPR o ochraně osobních údajů, přinášíme Vám nyní některé základní odpovědi na důležité otázky.

Přehled základních pojmů a informací vztahujících se k obecnému nařízení

Co znamená obecné nařízení o ochraně osobních údajů?

Obecné nařízení představuje aktualizovaný právní rámec ochrany osobních údajů v evropském prostoru, který bude od 25. května 2018 přímo stanovovat pravidla pro zpracování osobních údajů, včetně práv subjektu údajů (fyzické osoby). V českém právním prostředí tak obecné nařízení od 25. května 2018 nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů, který v současné době stanovuje povinnosti a práva při zpracování osobních údajů.

Proč muselo dojít k revizi právního rámce ochrany osobních údajů?

K revizi bylo přikročeno z toho důvodu, že současný právní rámec, založený směrnicí 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, již přestal odpovídat současné době, zejména pokud jde o prostředky, které jsou ke zpracování využívány a též i pokud jde o zpracování jako takové, které je daleko komplexnější, než bylo před několika desítkami let (např. v oblasti profilování, automatizace zpracování osobních údajů atd.) a tudíž je i rizikovější pro práva a svobody fyzických osob. Zároveň v jednotlivých zemích Evropské unie nebyla Směrnicí 95/46/ES dosažena požadovaná míra sjednocení právní úpravy, což správcům působícím ve více zemích činilo problémy.

Je obecné nařízení revolucí, tak jak jsem o něm několikrát slyšel hovořit?

V základních bodech obecné nařízení není revolucí, jelikož jde o kontinuitu se zmíněnou Směrnicí 95/46/ES, která jím bude zrušena. Je nutné si uvědomit, že od roku 2000 upravuje zpracování osobních údajů v České republice zákon č. 101/2000 Sb., o ochraně osobních údajů, který vychází ze zmíněné směrnice. Každá organizace by již tedy měla zpracovávat osobní údaje podle tohoto zákona. Za revoluci bychom mohli označit pouze přímou použitelnost obecného nařízení, což vyplývá z jeho charakteru, jakožto nařízení.

Kdo se bude muset obecným nařízením řídit?

Obecným nařízením se bude především, pokud jde o povinnosti, řídit subjekt, který provádí zpracování osobních údajů. Takový subjekt je nazýván správcem osobních údajů. Obecným nařízením se řídí i zpracovatel, což je subjekt, který pro správce osobní údaje zpracovává. Pokud jde o práva vyplývající z obecného nařízení, ta vyplývají fyzické osobě, což je subjekt údajů. Dále se obecným nařízením budou řídit i dozorové úřady, tj. i Úřad pro ochranu osobních údajů, který bude uplatňovat svěřené pravomoci za účelem plnění stanovených úkolů.

Musí se obecným nařízením řídit i drobný živnostník nebo malý internetový obchod?

Ano, pokud při jejich činnosti dochází ke zpracování osobních údajů, což z povahy věci zpravidla dochází (nejčastěji osobní údaje zákazníků – fyzických osob, či osobní údaje zaměstnanců nebo obchodních partnerů). Je však nutné si uvědomit, že obecné nařízení klade vyšší nároky především na subjekty, které zpracovávají osobní údaje ve velkém rozsahu či zvláštní kategorie osobních údajů, resp. pokud jsou osobní údaje hlavním bodem činnosti. To jsou například banky, telekomunikační operátoři, velké nemocnice atd.

Pokud při činnosti určitého subjektu dochází k běžné práci s osobními údaji nezbytnými např. k provedení služby či prodeji výrobku, lze zpravidla konstatovat, že obecné nařízení nepřináší rozdíly oproti současnému zákonu č. 101/2000 Sb., o ochraně osobních údajů. U těchto subjektů (malý internetový obchod, živnostník – opravář, mající klientelu z řad fyzických osob), které tedy neprovádí rozsáhlé či rizikové zpracování, je nezbytné zejména dodržovat zásady zpracování osobních údajů. Nutné je především sledovat legitimní účel, pro který byly osobní údaje shromážděny (např. uzavření

Na jaké činnosti obecné nařízení nedopadá?

Z působnosti obecného nařízení jsou vyloučeny činnosti fyzické osoby [viz článek 2 odst. 2 písm. c) obecného nařízení], při kterých jsou zpracovávány osobní údaje výlučně pro osobní či domácí činnost. Např. na zpracování osobních údajů pro účely tvorby rodinného rodokmenu se na fyzickou osobu, která tento rodokmen vytváří pro osobní potřebu, nevztahuje obecné nařízení.

Dále je z působnosti obecného nařízení vyloučeno zpracování prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. To je předmětem úpravy Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. Jelikož jde o směrnici, je nutné její provedení, které bude vesměs v adaptačním zákoně.

GDPR v otázkách a odpovědích

V následující kapitole Vám přinášíme některé odpovědi na dotazy, které jsou zveřejněny na stránkách Ministerstva vnitra. Věřím, že některé informaci budou pro Vás přínosné.

Právní titul

Jaký je právní titul pro zpracování osobních údajů v rámci podnětů a podání občanů vůči veřejné správě? Je to zákon č. 500/2004 Sb., správní řád, tedy je možno použít právní titul dle čl. 6 odst. 1 písm. c) GDPR?

Přijímání podnětů a stížností lze řadit pod právní důvody zpracování nezbytné pro plnění zákonem stanovené povinnosti.

Bude docházkový systém založený na použití otisků prstů a jednosměrného hashování, kdy nedochází k uchovávání samotných otisků prstů v databázi zaměstnavatele, v souladu s obecným nařízením o ochraně osobních údajů?

Obecné nařízení o ochraně osobních údajů v článku 9 odst. 1 zakazuje zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby. Podle článku 9 odst. 2 písm. b) se odstavec 1 nepoužije, pokud je zpracování nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů.

Podle článku 9. odst. 4 členské státy mohou zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování biometrických údajů. Tyto možnosti by členské státy měly mít i podle recitálu 53 obecného nařízení. Podle recitálu 91 by mělo být v případech, kdy se osobní údaje zpracovávají v návaznosti na zpracování biometrických údajů, vypracováno posouzení vlivu na ochranu osobních údajů.

Jaký bude výklad těchto ustanovení, zda bude za zpracování biometrických údajů považováno i vstupní použití otisků prstů, aniž by docházelo k jejich uchovávání v databázi správce, či zda bude takový postup po posouzení vlivu na ochranu osobních údajů považován při dodržení stanovených záruk za přípustný, není zatím zřejmé. Mělo by to být předmětem jednotného celoevropského přístupu k této problematice, o kterém bude Úřad informovat.

Podléhá požadavkům GDPR účetnictví (prodejní doklady, mzdová a personální agenda) a co je třeba posoudit při zabezpečení této agendy?

Obecné nařízení o ochraně osobních údajů (GDPR) se týká všech subjektů, které zpracovávají osobní údaje fyzických osob, například zaměstnanců či klientů. V rámci účetnictví se jedná o zpracování podle zvláštního zákona, kterým je zákon č. 563/1991 Sb., o účetnictví, a je tedy nezbytné pro splnění právní povinnosti, která se na správce vztahuje ve smyslu článku 6 odst. 1 písm. c) obecného nařízení.

Úřad pro ochranu osobních údajů doporučuje přihlédnout, v jakém stavu se nachází technika zvolená pro účel zpracování, provádět pravidelné testování a hodnocení účinnosti zavedených technických a organizačních opatření pro bezpečnost zpracování. Při posuzování vhodné úrovně bezpečnosti je třeba zohlednit zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených či jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Práva subjektu údajů

Pokud využiji své právo subjektu údajů na přístup k osobním údajům podle GDPR, do jaké lhůty mi správce bude muset zaslat informace?

Ve smyslu ustanovení čl. 12 odst. 3 obecného nařízení o ochraně osobních údajů je správce povinen poskytnout na žádost subjektu údajů dle článků 15 až 22 citovaného nařízení informace o přijatých opatřeních bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti.

Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další dva měsíce. Správci je uložena povinnost subjekt údajů o takovémto prodloužení informovat, a to do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad.

Na základě čl. 13 odst. 4 GDPR nemusí správce poskytovat subjektu údajů informace o jeho zpracovávaných osobních údajích za situace, že subjekt už tuto informaci má. Je platný a účinný právní předpis, na jehož základě jsou osobní údaje subjektu zpracovávány, dostatečnou informací pro tento subjekt a je tedy možné za této situace využít znění čl. 13 odst. 4 GDPR?

V daném případě může záležet na kontextu, ale obecně nelze považovat platný a účinný právní předpis za a priori zprošťující okolnost pro správce z povinnosti informovat subjekt údajů dle článku 13, resp. 14 obecného nařízení.

V jakém rozsahu musí správce poskytnout údaje na základě žádosti subjektu dle č. 15 GDPR za situace, kdy je tato žádost bez specifikace a je pojata obecně? Bude muset odpověď správce obsahovat i všechny osobní údaje z minulosti subjektu, které již správce nezpracovává?

Správce by měl vždy řádně posoudit přijatou žádost dle článku 15 obecného nařízení. Podotýkám, že v současné době zákon č. 101/2000 Sb., o ochraně osobních údajů, v § 12 obsahuje ekvivalent tohoto práva.

Pokud má správce pochybnosti o totožnosti osoby, která žádá o informace, může postupovat dle článku 12 odst. 6 obecného nařízení, tj. může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů (který podává žádost).

Pověřenec pro ochranu osobních údajů

Musí kulturní příspěvkové organizace kraje (muzea a galerie) zřizovat funkci DPO ve svých organizacích, když nedochází v dané organizaci k rozsáhlému zpracování osobních údajů (dle čl. 37 obecného nařízení)?

Neplatí, že by jen pouze z důvodu, že organizace byla založena subjektem, který musí mít pověřence, měla mít též pověřence. Jinými slovy u takto založených organizací je nutné zkoumat, zdali nemusí mít pověřence především dle článku 37 odst. 1 písm. b), c) obecného nařízení. Důležité je věnovat pozornost podmínkám, které musí nastat pro vznik této povinnosti (např. musí jít o hlavní činnost spočívající v rozsáhlém zpracování zvláštních kategorií osobních údajů či jít o hlavní činnost spočívající v rozsáhlém monitorování subjektů údajů).

Muzeum, galerie, knihovna – jejich činnost nespadá do vymezení v článku 37 odst. 1 písm. b) a c) obecného nařízení – zatímco například nemocnice, zřízená městem, bude muset mít pověřence, ale ne z důvodu, že ji založilo město, ale proto, že je její hlavní činností rozsáhlé zpracování zvláštních kategorií osobních údajů (o zdravotním stavu), tedy dle písmena c).

Krajské knihovny lze postavit na úroveň ostatním knihovnám, tj. nemusí mít pověřence, a to ani tehdy, pokud budou rozesílat pozvánky na jimi pořádané akce. Muzea, galerie či knihovny nemusí mít pověřence, pokud zpracovávají nezbytné osobní údaje v souvislosti s jejich oprávněnou činností, včetně osobních údajů zaměstnanců pro pracovněprávní účely či uspokojování potřeb členů nebo mají kamerový systém.

Jsme nezisková organizace – domov pro seniory s počtem 133 zaměstnanců. Musíme jmenovat pověřence pro ochranu osobních údajů?

Pověřenec pro ochranu osobních údajů je jedním z nových nástrojů ochrany osobních údajů, které zavádí obecné nařízení (GDPR) k datu své účinnosti od 25. května 2018. Počet zaměstnanců pro jmenování pověřence pro ochranu osobních údajů není rozhodný, jmenuje ho správce pouze za splnění jedné ze tří podmínek. Těmi jsou:

- zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;
- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Dle Vašeho popisu organizace se na Vás nevztahuje ani jedna ze tří podmínek, tedy pověřence pro ochranu osobních údajů mít nemusíte. Můžete si ho však zřídit dobrovolně, pokud uznáte, že zřízení pověřence pro Vás bude užitečné, v takovém případě by pověřenec měl mít odpovídající odborné znalosti práva v oblasti ochrany osobních údajů a schopnosti plnit úkoly stanovené v čl. 39 obecného nařízení.

I v případě, že pověřence jmenovat nebudete, je vítané mít v organizaci určenou osobu, která se bude ochraně osobních údajů věnovat.

Musí mít pověřenec pro ochranu osobních údajů nějakou certifikaci? Spousta firem certifikaci na DPO nabízí.

Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) nestanovuje certifikaci pověřence jako předpoklad výkonu funkce pověřence. Pověřenec tak certifikát mít nemusí a správce může jako pověřence vybrat i „necertifikovanou“ osobu, která disponuje dostatečným právním povědomím o ochraně osobních údajů a citovaném Obecném nařízení.

Není vyloučeno, že některé firmy „certifikaci“ pověřenců nabízejí, nicméně využití certifikace pověřence bude na dobrovolné bázi, a to jak ze strany pověřence, tak ze strany správce, který nemá povinnost vybírat certifikovaného pověřence.

Budou muset společenství vlastníků jednotek jmenovat pověřence pro ochranu osobních údajů?

Společenství vlastníků jednotek, jestliže provádějí pouze zpracování osobních údajů v souvislosti s činnostmi spočívajícími v zajišťování výkonu bytových spoluvlastnických práv a povinností tak, jak je upravuje zákon č. 89/2012 Sb., občanský zákoník (viz § 1158 a násl. občanského zákoníku), pověřence jmenovat nemusejí.

Co se rozumí pod pojmem „rozsáhlé zpracování a rozsáhlé systematické monitorování“? Je možno tyto pojmy vyjádřit nějak kvantitativně?

K výkladu pojmu „rozsáhlé zpracování a rozsáhlé systematické monitorování“, nejspíše myšleno ve vztahu k povinnosti jmenovat pověřence pro ochranu osobních údajů, doporučuji vycházet z vodítek pracovní skupiny WP29 k pověřencům. Vodítka jsou k dispozici na stránce.

Ve zmíněných vodítkách jsou tyto pojmy rozebrány.

Kdo bude kontrolovat pověřence pro ochranu osobních údajů, že vykonávají svou činnost řádně a s péčí odborníka? Bude to ÚOOÚ?

Obecné nařízení o ochraně osobních údajů stanovuje povinnost jmenovat pověřence vymezenému okruhu organizací. Primárně tak bude Úřad pro ochranu osobních údajů kontrolovat, zdali organizace, která má podle článku 37 odst. 1 obecného nařízení povinnost jej jmenovat, tak učinila. K institutu pověřence se však váží i další povinnosti, mimo jiné povinnost jmenovat pověřence na základě jeho profesních kvalit, zejména na základě jeho odborných znalostí práva a praxe v oblasti ochrany údajů a schopnosti plnit úkoly stanovené v článku 39 obecného nařízení. Součástí kontroly tak může být i kontrola plnění povinnosti dle článku 37 odst. 5 obecného nařízení. Ta by byla na místě především tehdy, pokud by zpracování, které provádí organizace se jmenovaným pověřencem, vykazovalo závažná pochybení a vznikaly by tak pochyby o odborné úrovni jmenovaného pověřence.

Posouzení vlivu na ochranu osobních údajů

Co je to „veřejně přístupný prostor“ definovaný v čl. 35 odst. odst. 3 písm. c) GDPR? Je to pouze místo, kde může v určitém okamžiku vstoupit neomezený počet osob, anebo jsou to i učebny ve školách a zkušebny v budovách orgánů veřejné správy?

Co se týče výkladu pojmu „veřejně přístupný prostor“ ve vztahu k článku 35 odst. 3 písm. c) Obecného nařízení, lze odkázat na vodítka pracovní skupiny WP29 k posouzení vlivu na ochranu osobních údajů, ve kterých je na straně 9 v poznámce pod čarou čl. 15 k tomuto pojmu uvedeno:
The WP29 interprets "publicly accessible area" as being any place open to any member of the public, for example a piazza, a shopping centre, a street, a market place, a train station or a public library.

Lze se tak přiklonit k názoru, že to budou jiné prostory než učebny či školy, ty zpravidla nebudou splňovat definici pojmu veřejně přístupný prostor. Veřejně přístupným prostorem je typicky např. nákupní obchodní centrum, ulice, vlaková stanice nebo veřejná knihovna. Tato vodítka je možné stáhnout na odkazu http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

Při zpracování osobních údajů, které jsou upraveny právním předpisem, není nutno provádět posouzení vlivu takového zpracování (viz čl. 35 odst. 10 GDPR a § 9 návrhu nového zákona). Vztahuje se toto zproštění povinnosti i na všechny zákony, u kterých nebylo v minulosti v rámci legislativního procesu provedeno posouzení vlivu na ochranu osobních údajů, tedy byly uvedeny v platnost a účinnost už před vydáním RIA?

Návrh adaptačního zákona, který je v současné době v legislativním procesu s pracovním názvem zákon o zpracování osobních údajů, obsahuje ustanovení, že před zahájením zpracování osobních údajů, které je upravené právním předpisem, není nutno provádět posouzení vlivu zpracování na ochranu osobních údajů.

Kodexy chování pro veřejnou správu

Budou vytvořeny kodexy chování dle čl. 40 GDPR pro veřejnou správu? Případně který orgán a kdy je vytvoří?

Předpokládá se, že kodexy chování budou fungovat především na sektorové úrovni, což je de facto i jejich účel, být nápomocny správcům se stejnými „problémy“.

Pokud jde o kodex chování pro veřejnou správu, šlo by již spíše o horizontální kodex a v tuto chvíli Úřad pro ochranu osobních údajů nemá informace, že by nějaký subjekt uvažoval o jeho vytvoření, ostatně je otázkou, zdali by bylo možné vytvořit kodex chování pro celou státní správu (musel by být s ohledem na pestrost státní správy velmi obecný, což by již odporovalo funkci kodexu chování jako takovému, který by měl být pro správce vodítkem právě ve specifických sektorových situacích).

Internetové obchody

Jak je to se souhlasy, resp. potřebují e-shopy ke zpracování osobních údajů souhlas zákazníků? A jak to bude s již získanými souhlasy? Znamená to, že obchodníky čeká povinnost získat tyto souhlasy znovu?
Bod 171 preambule obecného nařízení se zabývá přechodem souhlasů po datu použitelnosti obecného nařízení. K provozu internetového obchodu (pro účely plnění smlouvy) není nutné obstarávat souhlas se zpracováním osobních údajů. Každý provozovatel e-shopu musí vzít obecné nařízení (stejně tak jako dnes zákon č. 101/2000 Sb., o ochraně osobních údajů) v úvahu ve vztahu ke všem činnostem s osobními údaji, které provádí. Obstarávání souhlasu čeká ty správce, kteří musí ke zpracování osobních údajů mít souhlas a zároveň tento souhlas neodpovídá především podmínkám článku 7 obecného nařízení (např. byl presumován v obchodních podmínkách, aniž by subjekt údajů měl reálnou možnost uzavřít plnění i bez takto presumovaného souhlasu).

Pro úplnost je třeba upozornit, že pravidla pro používání cookies a zpracování osobních údajů za účelem elektronické reklamy, dosud upravená zvláštními předpisy (zákon č. 127/2005 Sb. a č. 480/2004 Sb.), budou ovlivněna přijetím dalšího předpisu EU, tzv. nařízení o e-privacy, jehož schválení lze očekávat v 2. pol. roku 2018.

Dopadá GDPR jen na některá, např. systematická zpracování osobních údajů nebo na všechny operace s osobními údaji?
Po obsahové stránce dosavadní definici zpracování osobních údajů obecné nařízení nemění, povinnosti zpracování osobních údajů se tak vztahují na nakládání s papírovými dokumenty a evidencemi, stejně jako na počítačové databáze a přenosy, tedy typické operace e-shopů s osobními údaji.

Bude řada provozovatelů e-shopů povinna jmenovat pověřence pro ochranu osobních údajů?
Běžný provoz e-shopů nedává důvod jmenovat pověřence pro ochranu osobních údajů. Povinnost jmenovat pověřence pro ochranu osobních údajů je pro určité organizace, resp. druhy zpracování stanovena v článku 37 odst. 1 obecného nařízení.

Jaké konkrétní náležitosti by měla obsahovat smlouva o zpracování osobních údajů mezi správcem osobních údajů (internetovým obchodníkem) a zpracovatelem (hostingovou či softwarovou společností)?
Smlouva o zpracování osobních údajů není novinkou, ale je již zahrnuta v zákoně o ochraně osobních údajů a to v § 6. obecné nařízení se vztahu správce – zpracovatel věnuje v článku 28. U smlouvy o zpracování osobních údajů by mělo být dbáno, aby především obsahovala náležitost dle návěstí odst. 3 článku 28 obecného nařízení (což už by měla obsahovat i dnes dle § 6 zákona o ochraně osobních údajů).

V ČR dosud nebyla přijata národní legislativa doplňující GDPR, znamená v tuto chvíli pro podnikatele s e-shopy nejistotu?

Obecné nařízení je komplexním právním předpisem, který nahradí zákon o ochraně osobních údajů. Povinnosti (i práva subjektu údajů) tak vyplývají z tohoto přímo použitelného předpisu EU a není třeba proto čekat na adaptační legislativu. Z dílčích věcí, které mohou adaptační předpisy blíže upravovat, lze za podstatnou pro podnikání na internetu považovat stanovení věkové hranice pro udělení souhlasu dítěte v souvislosti s nabídkou služeb informační společnosti.

GDPR předpokládá vytvoření a používání nejrůznějších vzorových dokumentů a kodexů, které mají správcům a zpracovatelům pomáhat při plnění právních povinností. Budou kodexy vydány Úřadem pro ochranu osobních údajů nebo jinými orgány, třeba formou nějakého předpisu?
Z obecného nařízení vyplývá předpoklad, že kodexy chování vytvoří asociace či sdružení zastupující správce ze stejné oblasti (např. bankovnictví, telekomunikace, cestovní kanceláře). Není vyloučeno vytvoření horizontálního kodexu např. pro internetové obchody. Není úkolem dozorového úřadu tyto kodexy vytvářet, ÚOOÚ však již k přípravě několika kodexů poskytl konzultace. Obecné nařízení nestanovuje povinnost kodexy vytvořit.

Připravujeme se na budoucí spuštění e-shopu. Budeme se muset registrovat i po nabytí účinnosti GDPR v květnu 2018? Bude podle GDPR odpovídat za data zákazníků provozovatel e-shopu nebo jeho pronajímatel, u kterého budou veškerá data uložena v databázi a webhostingu?

Pokud e-shop zpracovává osobní údaje v souvislosti s činnostmi spočívajícími v uzavření a plnění kupní smlouvy, vztahuje se na něj výjimka z oznamovací povinnosti podle § 18 odst. 1 písm. b) zákona č. 101/2000 Sb., která stanoví že: oznamovací povinnost se nevztahuje na zpracování, které správci ukládá zvláštní zákon, nebo je takových osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona."
S účinností obecného nařízení o ochraně osobních údajů (GDPR) 25. května 2018 bude oznamovací povinnost zrušena, obecné nařízení však klade na správce osobních údajů větší odpovědnost při posouzení rizik, která mohou pro subjekty údajů ze zpracování vyplývat a stanoví i některé nové povinnosti, např. ohlašování případů porušení zabezpečení osobních údajů Úřadu.
Za zpracování osobních údajů odpovídá nyní, stejně jako po nabytí účinnosti GDPR, primárně správce osobních údajů, kterým je provozovatel e-shopu, uzavírající smlouvy se svými zákazníky. Jestliže budou data uložena v databázi a webhostingu pronajímatele, bude pronajímatel v postavení zpracovatele, s nímž je třeba uzavřít smlouvu podle článku 28 odst. 3 GDPR. Zpracovatel je rovněž odpovědný za přijetí opatření k zabezpečení osobních údajů podle článku 32 GDPR.

Hotelnictví a cestovní ruch

Jak podle obecného nařízení postupovat při zapisování osobních údajů hostů ubytovacího zařízení do ubytovací knihy a ubytovací knihy cizinců pro účely cizinecké policie?
Pokud budete provádět zpracování, které Vám jako ubytovacímu zařízení ukládá zákon nebo jiná právní norma, bude se jednat o zpracování prováděné na základě právního důvodu uvedeného v čl. 6 odst. 1 písm. c) obecného nařízení (GDPR), tj. zpracování nezbytné pro splnění právní povinnosti, která se na správce vztahuje. Připojuji odkaz na stanovisko Úřadu k této věci, obsahově by se na něm nemělo nic zásadního měnit ani po nabytí účinnosti obecného nařízení:
https://www.uoou.cz/stanovisko-c-7-2012-evidence-ubytovanych-osob/d-1543/p1=1099

Doporučuji Vám prostudovat čl. 13 a 14 obecného nařízení týkající se povinnosti správce poskytovat subjektu údajů informace o prováděném zpracování. Dalším důležitým ustanovením je čl. 24 o odpovědnosti správce při zajištění bezpečnosti osobních údajů: s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Upozornit je třeba i na článek 32 Zabezpečení zpracování, hlavně z důvodu, že ve svém dotazu uvádíte, že někteří provozovatelé ubytovacích zařízení nechávají knihy hostů volně dostupné, aby se tam hosté sami zapisovali. To je z pohledu dnes platné právní úpravy i z pohledu obecného nařízení zcela nezodpovědné nakládání s osobními údaji hostů (subjektů údajů).

Ještě upozorním na čl. 30, kde je upraveno vedení záznamů o činnostech zpracování, sice se toto ustanovení netýká podniků či organizací, které zaměstnávají méně než 250 zaměstnanců, ledaže by zpracování, které provádí, představovalo riziko pro práva a svobody subjektů údajů (tím by v případě lázeňského zařízení bylo zpracovávání údajů o zdravotním stavu klientů, které by nebylo nahodilé, tj. jednalo by se o běžnou součást poskytované péče).

Sociální služby

Co nového bude GDPR znamenat pro nestátní neziskovou organizaci poskytující sociální služby podle zákona o sociálních službách?

Nařízení Evropského parlamentu a Rady 2016/679 (tzv. GDPR) zavedlo některé nové instituty, například institut tzv. pověřence. V oddílu 4 je stanoveno, v kterých případech správce a zpracovatel jmenují pověřence, jeho postavení a úkoly.

Dalšími novými instituty jsou například:

- posouzení vlivu na ochranu osobních údajů podle čl. 35 GDPR,
- předchozí konzultace podle čl. 36 GDPR,
- povinnost vést záznamy o činnostech zpracování podle čl. 30 GDPR.

Tyto povinnosti se však nevztahují na každého správce a Vy sami si musíte posoudit, které z těchto činností budete aplikovat.

Úřad nezná podrobnosti, ale o radu či pomoc při uvádění do souladu Vašeho zpracovávání osobních údajů fyzických osob s GDPR můžete také požádat Ministerstvo práce a sociálních věcí, které má povinnost od 25. května 2018 pověřence mít podle čl. 37 odst. 1 písm. a) GDPR, když se jedná o zpracovávání osobních údajů orgánem veřejné moci.

Pokud v současné době zpracováváte osobní údaje na základě právního důvodu uvedeného v § 5 odst. 2 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (to znamená, že zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje, a je uvedena ve zvláštním zákoně, kterým může být i zákon o sociálních službách), právní důvod zpracování a základní povinnosti správce zůstávají ve své podstatě stejné i po nabytí účinnosti GDPR.

Ostatní

Jak může zpracovatel v souladu s GDPR užívat služeb dalších subdodavatelů při zpracování osobních údajů?

Subdodavatelé by byli v režimu čl. 29 obecného nařízení, který stanoví, že zpracovatel a jakákoliv osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, může tyto osobní údaje zpracovávat pouze na pokyn správce, ledaže jí jejich zpracování ukládá právo Unie nebo členského státu.

Pokud tyto osoby jednají z pověření správce a na jeho pokyn, mohou mít přístup k osobním údajům.

Desatero zpracování pro správce

Desatero zpracování pro správce je zestručnění základních pravidel ochrany osobních údajů, využitelné malými správci údajů, živnostníky či menšími podniky, coby základní jednoduchý návod, jak zacházet s osobními údaji.

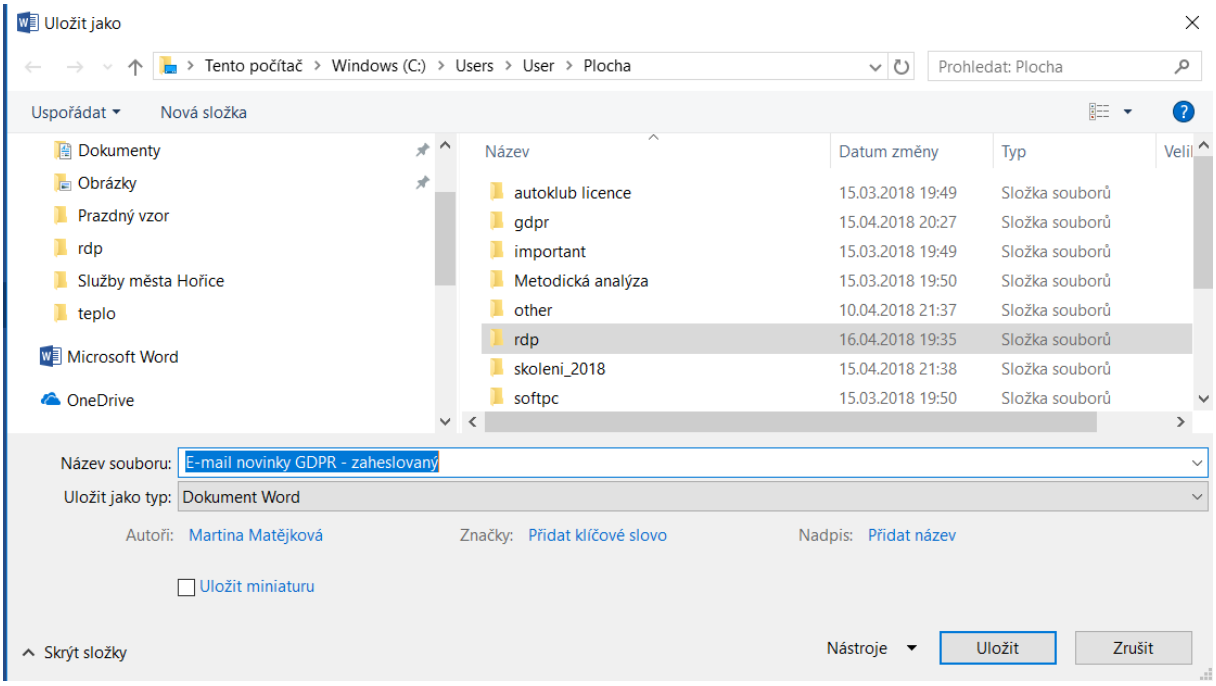
1. Zpracování údajů, ať je nařízeno zákonem, prováděno z vůle správce nebo po dohodě či se souhlasem dotčených osob, **musí být legitimní** a nesmí být v rozporu s právními předpisy či morálkou.
2. Každé zpracování údajů musí být **založeno na některém ze základních důvodů** (právních titulů pro zpracování), nejčastěji se jedná o smluvní plnění, výkon právních povinností či plnění zákonného oprávnění, výkon veřejné moci nebo zpracování na základě souhlasu dotčené osoby.
3. Každý, kdo shromažďuje, dále zpracovává a uchovává osobní údaje, musí jasně vymezit (stanovit a být schopen vysvětlit) sledovaný záměr – účel **zpracování údajů.**
4. Všechny způsoby a formy, rozsah zpracování a doba uchovávání údajů musí být **vždy přiměřené účelu zpracování.**
5. Pokud detaily zpracování stanoví veřejnoprávní předpis, nelze se od nich většinou odchýlit. Každé zpracování ve veřejném sektoru musí mít **jasný zákonný podklad**, takové zpracování nelze nahradit souhlasem se zpracováním údajů.
6. Správce i zpracovatel osobních údajů musí osobní údaje **patřičně zabezpečit** a chránit organizačními a technickými opatřeními – v míře odpovídající rizikovosti zpracování.
7. Zpracování by mělo být vůči dotčeným fyzickým osobám prováděno **férově, korektně a transparentně**. Informace o zpracování poskytované subjektu údajů musí být **zřetelné, jednoznačné a srozumitelné, v rozsahu odpovídajícímu konkrétní situaci.**
8. Zpracování **nesmí nadměrně zasahovat do soukromí**. Správci mohou volit různé přiměřené prostředky zpracování, v případě moderních technologií jsou však povinni zvážit nová rizika i dopady do soukromí jednotlivců. Zejména musí uvážit důvodnost a oprávněnost každého sdílení či zveřejnění negativních či jinak citlivých údajů.
9. Po naplnění účelu zpracování je dána povinnost osobní údaje **zlikvidovat**. Delší dobu uchování mohou stanovit zákonná pravidla pro archivaci nebo zvláštní využívání údajů (státní statistická služba, nemocenské a důchodové pojištění apod.).
10. V rámci EU je v každé členské zemi zaručena unifikovaná ochrana osobních údajů, kterou stanoví obecné nařízení (GDPR). Předávat osobní údaje mimo Evropskou unii lze jen za splnění dodatečných pravidel nebo za určitých okolností, jako je např. plnění smlouvy se subjektem údajů.

Zdroj: webové stránky Úřadu pro ochranu osobních údajů

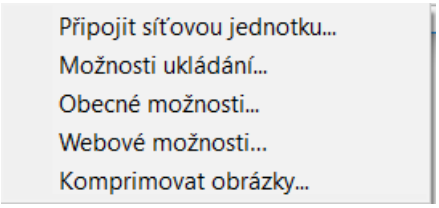
Zabezpečení odesílaných příloh elektronickou poštou – doplnění souboru heslem

Jednou z variant, jak mohou pracovníci organizace zabezpečit elektronický soubor pro jeho zaslaní elektronickou poštou příjemci, tak, aby nedošlo k jeho neoprávněnému zpracování, je možnost doplnění hesla pro otevření takového souboru.
Tuto funkci podporují například kancelářské programy MS Word nebo MS Excel, ale i jiné. V následujícím návodu si popíšeme doplnění hesla k elektronickému souboru v prostředí MS Office.

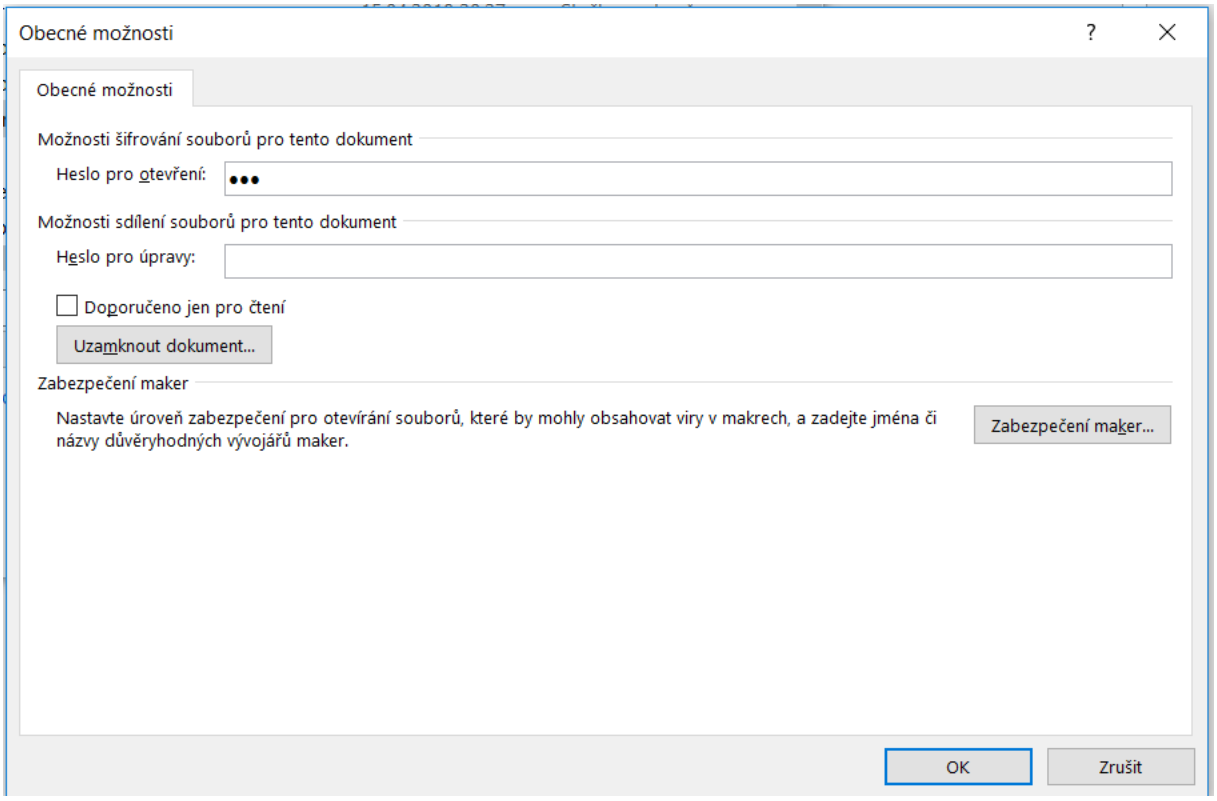
1. Vytvořený soubor uložíme přes funkci „Uložit jako“. Při ukládání zadáme název souboru s odlišným názvem, než je původní, který si ponecháme ve svém počítači (tento zpravidla nebudeme doplňovat heslem pro jeho otevření).
2. Zvolíme nabídku „Nástroje“ a zde vybereme funkci „Obecné možnosti“.
3. V údaji „Heslo pro otevření“ doplníme heslo, kterým chceme zabezpečit soubor pro jeho zaslání elektronickou poštou.
4. Heslo, které doplníme do souboru, zašleme příjemci jinou cestou než formou elektronické zprávy (například SMS atd.)



Obrázek 1: Uložení souboru pod jiný název ve svém PC



Obrázek 2: Výběr nabídky „Nástroje“ a zde zvolení funkce „Obecné možnosti“



Obrázek 3: Doplnění hesla do údaje „Heslo pro otevření“ a potvrzení tlačítkem „OK“

Nabídka služeb GDPR

Naší prioritou je dodávat našim zákazníkům kompletní služby. Z tohoto důvodu Vám nabízíme poskytování služeb pro řešení GDPR.
Rádi Vám umíme nabídnout:

- Zpracování úvodního **vnitřního auditu** k evidenci, uchovávání a zabezpečení veškerých informací o fyzických osobách, a to jak v elektronické, tak i v listinné podobě
- na základě tohoto auditu je zpracována **vnitropodniková směrnice** k nakládání s osobními údaji podle nařízení GDPR, která popisuje jednotlivé části v informačních systémech a evidenci dokumentů ve Vaší společnosti a navrhujeme taková řešení, která povedou k zajištění vyšší bezpečnosti dat o fyzických osobách
- toto by měl být začátek naší spolupráce. Doporučuji revizi vnitropodnikové směrnice vždy za určité období (rok asi ideální), kdy se provedou inventarizace změn proti předchozímu období a vyhodnotí se provedené změny
- **školení** všech pracovníků společnosti, kteří přicházejí do styku s osobními údaji subjektu údajů
- s každým klientem k tomuto uzavíráme smlouvu pro služby „**Pověřence pro ochranu osobních údajů“**, kde Vám garantujeme zajištění komplexního servisu k GDPR včetně metodické podpory. Tato služba je standardně bez žádného paušálního poplatku.

- v případě, že by ve Vaší společnosti došlo k incidentu se ztrátou osobních dat a byli jste za tuto chybu vyšetřování, nabízíme i spolupráci při řešení těchto situací. Nejsme však právníci tak, abychom Vás zastupovali u případného soudu. Věřím, že s naší pomocí se těmto událostem však vyhnete.

Ceník nabízených služeb

GDPR – vnitropodniková směrnice	7.000,00 Kč
Práce spojené s lokalizací směrnice na podmínky Vaší společnosti	900,00 Kč
Odborné školení pracovníků společnosti v oblasti ochrany osobních dat	1.200,00 Kč
Cestovní výdaje při osobních návštěvách	9 Kč/km + 450Kč/hod strávený čas na cestě
Služby „Pověřence pro ochranu osobních dat“	Bez paušálního poplatku hodinovou sazbou

NA ZÁVĚR

Pevně věříme, že informace, které jsme Vám poskytli v tomto našem novém magazínu, jsou pro Vás užitečné a praktické.
Za celý kolektiv pracovníků firmy Vám přeji hodně sil do následujících měsíců.

Tomáš Urban
ředitel společnosti

Softbit software, s.r.o.
Nad Dubinkou1634
516 01 Rychnov nad Kněžnou
Tel.: 494 532 202, 494 534 354; fax: 494 377 63
e-mail: softbit@softbit.cz
www.softbit.cz