GDPR & ERP Vision[32]

(General Data Protection Regulation)

Ver. 1

Obsah dokumentu

1. Úvodem

Vážení uživatelé informačního systému Vision[32]. V květnu 2016 bylo zveřejněno nařízení Evropského parlamentu a Rady EU o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Od té doby běží pro zpracovatele a správce dvouletá lhůta, po kterou jsou povinni svá zpracování osobních údajů uvést do souladu s tímto obecným nařízením. Obecné nařízení v současné době platné a jeho účinnost nastane 25. května 2018. K tomuto dni bude nařízení vymahatelné, tedy k tomuto dni musí být všechny subjekty již připraveny. GDPR se týká všech subjektů, které zaměstnávají alespoň jednoho zaměstnance, ukládají informace o zákaznících, občanech či pacientech, pracují s údaji v marketingové databázi, používají bezpečnostní kamery apod., tedy se dá s jistotou tvrdit, že se týká všech uživatelů ERP Vision[32].

Veškeré informace k nařízení jsou velmi obšírně zpracovány na webu Úřadu pro ochranu osobních dat. Naleznete zde jak překlad nařízení, příručku, časté otázky a odpovědi, tak i pokyny pracovní skupiny WP29, která jakožto nezávislý poradní orgán Evropské komise vydává pokyny a stanoviska. Další web, který velmi konkrétně vykládá GDPR pro malé a střední podniky je AMSP ČR a ČAOOÚ – GDPRBEZOBAV.CZ, kde naleznete doporučené postupy implementace a spoustu inspirace, jak se připravit.

Vhledem k tomu, že se účinnost nařízení blíží, předkládáme Vám tento dokument, ve kterém jsou popsány nové funkčnosti Vision[32] a možnosti, jak celou agendu GDPR vést a evidovat přímo v ERP Vision[32] ve spisové službě a nástrojích pro evidenci školení. Dále předkládáme informace o připravovaných nástrojích, již implementovaných funkcích a postupech, které vám mohou pomoci se s novými povinnostmi vypořádat.

Vision Praha s.r.o.
Všechromy 59
251 63 Strančice

Hodolanská 35
772 00 Olomouc

www.vision.cz
+420 585 313 130
vision@vision.cz

2. Stručný popis řešených oblastí

1) **Přístupová práva**:
   a) Změna všech hesel. Nyní lze řešit skriptem na úrovni správce, v následující verzi Vision[32] bude tato možnost pro administrátora přístupná jako funkce.
   b) Zajištění odolnosti a bezpečnosti hesla uživatelů Vision[32].
   c) Nové funkce umožňující řešit přístupy k tabulce kontaktů (i zaměstnanců) novým přístupem, který zajišťuje, dle několika úrovní, pseudonymizaci osobních dat.

2) **Zajištění důvěrnosti, integrity, dostupnosti a odolnosti systému**.
   a) Virtualizace serverů a systémy zálohování.
   b) Bezpečnostní schopnosti databáze, bezpečnostní politiky na serverech; veškerá data jsou umístěna v databázovém souboru.
   c) Neměnnost odesílaných dokumentů z Vision[32]. Odesílání dokumentů (PDF, ISDOC) z Vision[32] s elektronickým podpisem.
   d) Šifrování – uložení PDF s heslem.

3) **Analýza pro mapování stavu**
   a) Výpis údajů z databáze, kde všude se ve Vision[32] osobní data nachází.
   b) Ucelená dokumentová databáze pro pověřence či osoby určené.
   c) Nový nástroj Vision[32] k výpisu firem, které mají DIČ, jež může obsahovat rodné číslo a nejsou označeny jako fyzické osoby.
   d) Výpis fyzických osob, u kterých již není právní důvod k evidenci jejich osobních údajů.
   e) Možnost záznamu uděleného souhlasu se zpracováním osobních údajů.

4) **Řízení rizik a incidentů**.
   Řízení a záznamy incidentů. Neshody a jejich evidence, napojení na workflow. Hotová a odzkoušená aplikace přímo ve Vision[32].

5) **Směrnice GDPR**
   a) Jejich evidence.
   b) Změnová řízení.
   c) Vedení záznamů o zpracování osobních dat.
   d) Lhůta uchování osobních dat.

6) **Souhlasy se zpracováním osobních dat**:
   a) Evidence souhlasů (doložitelnost).
   b) Webová aplikace pro žádosti o souhlas se zpracováním osobních údajů.

7) **Evidence zpracovatelských smluv**.

8) **Školení zaměstnanců**.
   a) Záznamy školení pro prokázání dozorovému úřadu.
   b) Plán školení.

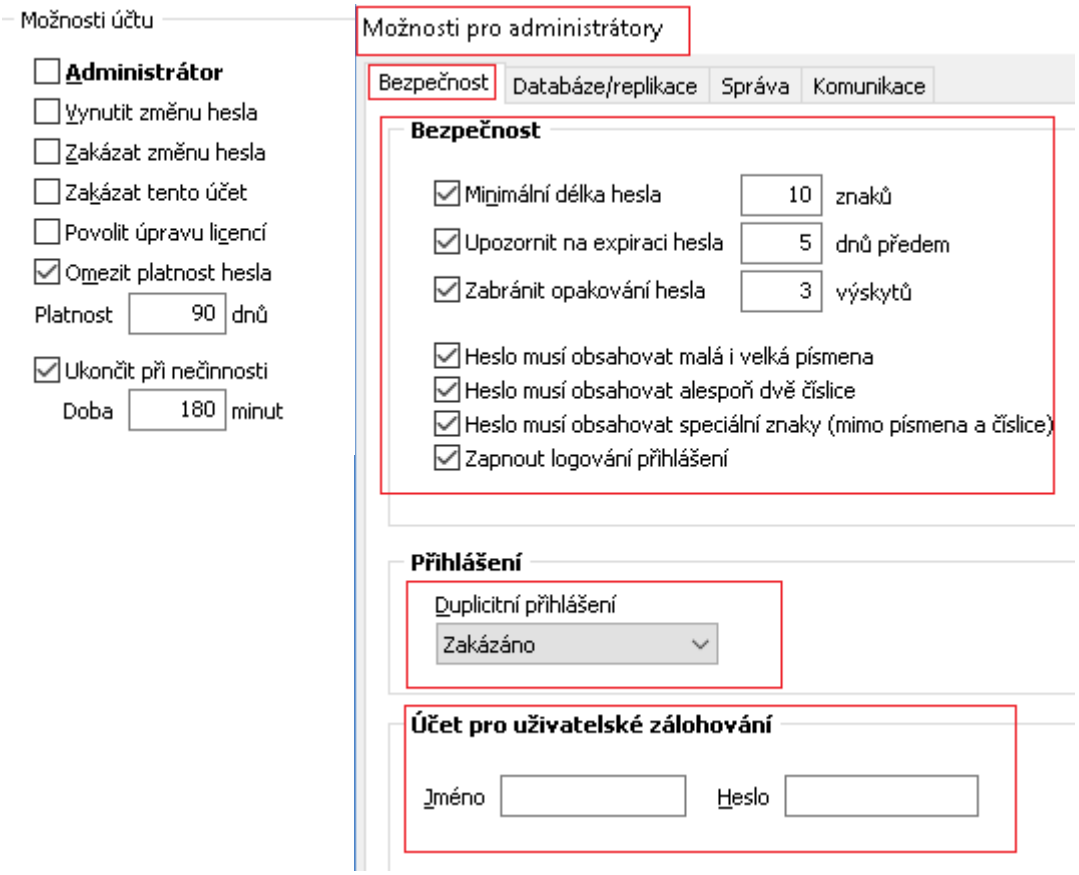
9) **Evidence osobních údajů a dat**
   a) Výmaz – anonymizace osobních dat na žádost či při prekluzi možnosti evidence z právního důvodu.
   b) Anonymizace části údajů, kde není právní důvod k evidenci a na žádost.
   c) Výpis evidence osobních dat na žádost subjektu osobních dat.

Vision Praha s.r.o.
Všechromy 59
251 63 Strančice
Hodolanská 35
772 00 Olomouc
www.vision.cz
+420 585 313 130
vision@vision.cz

3. Podrobněji k jednotlivým oblastem

(budete-li potřebovat podrobnější informace, neváhejte se na nás obrátit)

Přístupová práva



Změna hesel

Nastavit odolná hesla a v číselníku uživatelů mít aktivní jen ty, kdo s databází pracují. Je nutné poznamenat, že odolnost samotné databáze je zajištěna použitím databázového serveru SAP SQL Anywhere s plnohodnotným zabezpečením přístupu k datům. Je ale nutné zajistit, aby autentizovaný přístup jednotlivých uživatelů k databázi byl zajištěný odolným a nezneužitelným heslem. V číselníku uživatelů tedy bude nutné uživatelem s administrátorskými právy smazat nebo zakázat přístupová práva pro uživatele, kteří ve Vašem podniku již nepracují a účty, které nejsou využívané. Hesla ve Vision[32] nejsou ukládána, je uložen pouze tzv. hash hesla. Nutné je také zvážit, zda je nutné mít v databázi více jak jednoho administrátora. V této souvislosti upozorňujeme, že každý administrátor – tedy mimo jiných privilegií – může provést uživatelsky zálohu databáze, což by měl být řízený proces se zajištěním proti zneužití. Aby bylo možné zajistit odolnost hesel ostatních uživatelů, je možné donutit uživatele při dalším přihlášení změnit heslo. Je to nová funkce. Před tím, je však nutné administrátorsky nastavit funkci zajišťující odolnost hesla.

Odolnost a bezpečnost hesla

U každého uživatelského účtu lze omezit platnost hesla a nastavit odpojení od databáze při nečinnosti. Odolnost hesla je možné nastavit funkcí Možnosti programu - sdílené, záložka Ostatní Pro administrátory - Možnosti - záložka Bezpečnost. Můžete nastavit minimální délku hesla, pokud u uživatele omezíte platnost hesla, je možné určitý počet dnů před expirací na to uživatele upozornit a také zabránit opakování hesla. Pro odolné heslo lze mimo délky nastavit nutnost zadat malá i velká písmena, dvě číslice a speciální znaky. Pro sledování přihlášení zapnout logování. V každém případě doporučujeme zakázat duplicitní přihlášení.

Zálohování databáze smí provádět uživatel s právy administrátora. Pokud je nutné, aby zálohování prováděl i jiný uživatel, je možné přidělit mu ve vlastnostech účtu oprávnění gDBACKUP a nastavit účet pro zálohování. Doporučujeme však nastavit zálohování systémově a tuto funkci nepoužít.

A nakonec je nutné poučit uživatele, jak se chovat při zadávání hesla.

Kontakty a jejich evidence

Hlavní databázovou tabulkou kontaktů je tabulka gfkontakt. V této tabulce se nacházejí osobní data. Jedná se o data zaměstnanců, referentů, odpovědných osob za podaná přiznání a dalších, snahou je, aby existovala jedna tabulka kontaktů, ke které budou přiřazeny úrovně přístupu podle uživatelských skupin (následně rolí) a případně uživatelů (sloupec DBA.GUSERS.gdpr_level). V tom okamžiku je možné zakázat SELECT na tabulku kontaktů (DBA.GFKONTAKT) a zobrazení dat se bude řídit výhradně úrovněmi nastavených „GDPR úrovní". Veškerá zobrazení dat budou nadále prováděna procedurami, které dle přiřazené úrovně zobrazí jednotlivá pole s osobními daty. Takto bude zajištěn přístup pseudonymizací obecně k osobním datům napříč Vision[32].

Pokud budete chtít tyto úrovně GDPR využívat, obraťte se na nás se žádostí o prověření vašich uživatelsky definovaných sestav, browserů, přizpůsobení, pluginů apod. My vám prověříme vaše nastavení tak, abyste se nedostali do potíží s nedostupností jednotlivých částí systému.

Osobních dat zákazníků fyzických osob se tato funkce netýká, popis ochrany pro GDPR viz níže (označení v číselníku firem v položce Typ: Fyzická osoba plátce nebo Fyzická osoba neplátce).

Zajištění důvěrnosti, integrity, dostupnosti a odolnosti systému

Virtualizace serverů a systémy zálohování

Doporučujeme Vision[32] provozovat na virtualizovaných serverech, naše společnost vám nabízí jak možnost uložení vaší databáze v cloudu jako službu, tak i pomoc s virtualizací vašich serverů. Systém zálohování je nutné revidovat tak, aby bylo zřejmé, jakým způsobem se zálohování provádí, kde jsou záložní kopie dat uloženy a kdo k nim má přístup. **Společnost Vision Praha tyto služby nabízí**.

Bezpečnostní schopnosti databáze

ERP Vision[32] je dvouvrstvá (u web částí třívrstvá) aplikace, která pro správu dat využívá databázový server SAP SQL Anywhere. Architektura databáze a její bezpečnostní nástroje jsou popsány přímo na serveru společnosti SAP (https://www.sap.com/products/sql-anywhere.product-capabilities.html#product-capabilities). Jedná se o plnohodnotnou SQL databázi, s plnohodnotným zabezpečením přístupu k datům.

Přístup do databáze je strukturovaný. Databáze samotná je fyzicky tvořena jedním nebo více soubory, jejichž obsah a struktura nejsou přímo čitelné. Databáze samotná může mít nastavené až 128bitové

Vision Praha s.r.o.
Všechromy 59
251 63 Strančice
Hodolanská 35
772 00 Olomouc
www.vision.cz
+420 585 313 130
vision@vision.cz

kryptování. Soubory databáze obsluhuje databázový server a fyzické umístění databázových souborů nemusí být pro uživatele vůbec přístupné (nastavuje se stupněm oprávnění v rámci souborového systému).

K databázi může přistupovat pouze definovaný uživatel. Seznam a práva uživatelů se nastavují uvnitř databáze, neboli pouze jiným oprávněným uživatelem. Uživatelé se autentizují uživatelským jménem a heslem, jehož sílu lze administrátorsky vynutit. Využít lze rovněž autentizace uživatele centrálním síťovým poskytovatelem (doménovým serverem).

Databáze je z pohledu citlivých dat rozdělena na tabulky a pohledy. Mimo tyto zmíněné objekty obsahuje databáze i další objekty určené k práci s daty. Tabulky jsou vzájemně relačně svázány, ale přístup je každému uživateli definován ke každé tabulce nebo pohledu samostatně. Přístup je standardně rozdělen na práva „vkládat", „měnit", „mazat" a „prohlížet".

Z hlediska bezpečnosti citlivých údajů bude tedy nutno revidovat pouze přístupová práva uživatelů k citlivým tabulkám. Seznam těchto tabulek je uveden v tomto dokumentu pod bodem 3. Také vám poskytneme nástroje na vypsání seznamu uživatelů, kteří k daným tabulkám mají jakýkoliv přístup.

Administrátor by měl dále zajistit kontrolovaný přístup k databázi samotné.

Neměnnost odesílaných dokumentů z Vision32

ERP Vision32 umí odesílat PDF dokumenty podepsané elektronickým podpisem, stejně tak umí i daňové doklady odesílat v podepsaných souborech ISDOC. Takto lze zajistit neměnnost souborů při přenosu. U vydaných faktur je popis od roku 2016 zde: Elektronická fakturace. Nastavení elektronického podpisu pro hlášení a daňová hlášení je samostatné. Nastavení elektronického podpisu pro ostatní PDF soubory je v menu konfigurace – možnosti programu osobní – tisk/export.

Šifrování – uložení PDF s heslem

Soubory PDF umí Vision32 odesílat s autentizací heslem, to lze například využít pro odesílání výplatních lístků, heslo má každý zaměstnanec své, uložené v ERP Vision32. Nastavení v menu programu konfiguraci – možnosti programu osobní – tisk/export.

Analýza a mapování stavu

Přizpůsobení se obecnému nařízení (GDPR) bude u všech uživatelů Vision32 začínat provedením analýzy – mapováním stavu pro posouzení rizik. Jmenovaný pověřenec či osoba vedením k tomu určená bude muset trvat na provedení analýzy a auditu, ze kterého vzejdou směrnice, řízení rizik,... Evidence analýz a auditů a dalších dokumentů bude mimo jiné nezbytné jako důkazní prostředek v případě kontrol které mimo jiné mohou vzejít od povinného ohlašování případů porušení zabezpečení osobních údajů podle GDPR.

Výpis umístění osobních dat v databázi ERP Vision32

Pro provedení analýzy Vision32 předkládá seznam databázových tabulek, kde se osobní data zpracovávají, a to zde: GDPR-tabulky-osobní_data.

Ucelená dokumentová databáze pro pověřence či osoby určené. Řízení rizik a incidentů. Průběžná evidence dle GDPR.

ERP Vision32 má připravenou kompletní aplikaci spisové služby, ve které lze evidovat veškeré dokumenty včetně napojení na workflow. **Popis služby naleznete v dokumentu GDPR a směrnice.**

Vision Praha s.r.o.
Všechromy 59
251 63 Strančice
Hodolanská 35
772 00 Olomouc
www.vision.cz
+420 585 313 130
vision@vision.cz

Výpis firem s DIČ v podobě RČ – nová funkce

Výpis všech osob z číselníku firem, které lze považovat za fyzické osoby, a nejsou takto v číselníku obchodních partnerů označeny, bude k dispozici ve verzi 187. Cílem je pomoci s identifikací fyzických osob podnikajících – plátců DPH tak, abyste si mohli udělat pořádek v číselníku, aby bylo možné zjišťovat právní důvod evidence osobních dat podnikajících fyzických osob.

Výpis fyzických osob k anonymizaci – nová funkce

Výpis fyzických osob, u kterých již není právní důvod k evidenci jejich osobních údajů, provede nová funkce ve verzi 187, na základě tohoto výpisu bude možné přejít k anonymizaci evidovaných údajů u těchto odběratelů a dodavatelů.

Evidence souhlasů se zpracováním osobních údajů

Možnost záznamu uděleného souhlasu se zpracováním osobních údajů. Ve Vision[32] budou funkce umožňující, jak o souhlas se zpracováním osobních dat požádat, tak i evidence udělených souhlasů.

Souhlas se zpracováním osobních dat

Evidence souhlasů (doložitelnost)

V tabulce kontaktů bude možnost označení uděleného souhlasu s odkazem na příslušný dokument souhlasu, který budete mít možnost ukládat do databáze.

Webová aplikace pro žádosti o souhlas

Žádost o souhlas se zpracováním osobních dat bude možné z kontaktů ve Vision[32] posílat přímo prostřednictvím webové aplikace kterou společnost Vision nyní vyvíjí. Prostřednictvím vámi definovaných textů souhlasů ve spisové službě uložených přímo z Vision[32] bude možné odeslat žádost o udělení souhlasu a obdržený souhlas poté evidovat (vzhledem k požadavku doložitelnosti).

Evidence zpracovatelských smluv

Zpracovatelské smlouvy je možné evidovat přímo u obchodních partnerů, nebo ve spisové službě v samostatné číselné řadě.

Školení zaměstnanců

Záznamy školení pro prokázání dozorovému úřadu

V ERP vision[32] je už nyní evidence provedených školení, další funkčností bude evidence a plán hromadných školení.

Plán školení

Plán školení bude součástí Vision[32] – modul personalistiky.

Vision Praha s.r.o.
Všechromy 59
251 63 Strančice
Hodolanská 35
772 00 Olomouc
www.vision.cz
+420 585 313 130
vision@vision.cz

Evidence osobních údajů a dat

Výmaz – anonymizace osobních dat

Výmaz – anonymizace osobních dat na žádost či při prekluzi možnosti evidence z právního důvodu. ERP Vision[32] bude obsahovat ve verzi 187 novou funkci, která zajistí u dokladů vymazání polí s osobními daty.

Anonymizace části údajů

Anonymizace části údajů, kde není právní důvod k evidenci a na žádost. Zaměstnanci, kteří ukončí pracovní poměr, budou mít nově možnost požádat o výkaz údajů, které ze zákona firma nemusí evidovat. Nová funkce Vision[32] tento výmaz zajistí.

Výpis evidence osobních dat na žádost

Výpis evidence osobních dat na žádost subjektu osobních dat. Nová funkce ve verzi 187, která zajistí výpis všech oblastí, kde jsou osobní data v databázi Vision[32] evidována.

Vision Praha s.r.o.
Všechromy 59
251 63 Strančice

Hodolanská 35
772 00 Olomouc

www.vision.cz
+420 585 313 130
vision@vision.cz

4. Co vám ERP Vision32 vzhledem ke GDPR nabízí již dnes

V předchozím textu je popsána sada funkčních vlastností, které budou k dispozici v nové verzi ERP Vision32, tedy v budoucnu. Nicméně již dnes náš informační systém disponuje řadou funkcí a nástrojů, které vám umožňují nastartovat ihned kroky vedoucí k souladu celé agendy zpracování dat vzhledem ke GDPR. Jsou to nástroje jak technologické, vedoucí ke změnám v IT systémech a jejich zabezpečení, tak i softwarové, které vám umožňují započít změny v interní i externí dokumentaci anebo ve vlastních procesech.

Možnost migrace vašeho systému do „cloudu"

Provoz serveru v cloudu mimo mnohých bezpečnostních politik též řeší například záležitosti zálohování dat, přístupů k systému, fyzického zabezpečení dat a aktualizací operačních systémů. Migraci vašeho systému na virtuální server v „cloudu" vám na základě poptávky nabídneme jako komplexní službu.

Evidence zpracovatelských smluv.

Zpracovatelské smlouvy je možné evidovat přímo u obchodních partnerů, nebo ve „spisové službě" v samostatné číselné řadě.

Školení zaměstnanců

Záznamy školení pro prokázání dozorovému úřadu. V ERP Vision32 je už nyní evidence provedených školení, další funkčností bude evidence a plán hromadných školení.

Plán školení bude součástí modulu personalistiky.

Neměnnost odesílaných dokumentů z Vision32

ERP Vision32 umí odesílat PDF dokumenty podepsané elektronickým podpisem, stejně tak umí i daňové doklady odesílat v podepsaných souborech ISDOC. Takto lze zajistit neměnnost souborů při přenosu. U vydaných faktur je popis od roku 2016 zde: Elektronická fakturace. Nastavení elektronického podpisu pro hlášení a daňová hlášení je samostatné.

Nastavení elektronického podpisu pro ostatní PDF soubory je v menu konfigurace – možnosti programu osobní – tisk/export.

Systém umožňuje odeslat PDF soubory s „autentizací heslem". To lze využít například pro odesílání výplatních lístků, kdy každý zaměstnanec má své heslo uložené ve Vision32.

Nastavení v menu programu konfiguraci – možnosti programu osobní – tisk/export.

Evidence rizik

Agenda „Evidence rizik" je hotovou funkcionalitou ERP Vision32 a její instalací a zavedením dosáhnete plnohodnotné kontroly nad evidovanými riziky, odpovědnostmi, opatřeními a úkoly plynoucími z řešení rizik. Součástí aplikace je též evidence neshod (incidentů), které též umožňuje lepší kontrolu nad zjištěnými neshodami a kontrolu nad nastavenými opatřeními pro eliminaci neshod. Nabídku funkce pro „Řízení neshod" vám na základě poptávky zpracujeme podle individuálních potřeb.

Vision Praha s.r.o.
Všechromy 59
251 63 Strančice

Hodolanská 35
772 00 Olomouc

www.vision.cz
+420 585 313 130
vision@vision.cz

Spisová služba

Spisovou službu můžete využít k celé řadě potřebných evidencí s mimo jiné i k evidenci a správě směrnic (více viz dokument GDPR a směrnice).

Správa řízených dokumentů nepodléhajících změnám:

Smlouvy (dodavatelské, odběratelské).
Korespondence, dohody, udělené souhlasy.
Revize.
Zprávy.
atd.

Správa (včetně pravidelného přezkoumání a změnového řízení) řízených dokumentů podléhajících změnám:

Směrnice, metodické pokyny, návody.
Vzory smluv a jiné vzory.
Šablony a design manuály.
atd.

Vzhledem k interní dokumentaci GDPR to mohou být:

Záznamy zpracování.
preDPIA, DPIA.
Dokumentace dob zpracování.
Zpracování v rámci interních procesů.
Intragroup datových toků
atd.

Workflow (Procesy)

Schvalovací postupy pro jednotlivé třídy dokumentů (více viz dokument GDPR a směrnice). Je vhodné spojit se Spisovou službou.

Vision Praha s.r.o.
Všechromy 59
251 63 Strančice
Hodolanská 35
772 00 Olomouc
www.vision.cz
+420 585 313 130
vision@vision.cz

5. Formálně-právní kroky ve vztahu k ERP Vision[32]

Mít splněny požadavky dle GDPR je v zásadě odpovědností každého jednoho podniku, tzn. z pohledu ERP Vision[32] je na uživatelích našeho informačního systému. Ale je ze strany uživatelů ERP Vision[32] legitimní očekávat, že tento softwarový nástroj bude zmíněné evropské nařízení podporovat a že bude uživatelům nápomocen je dodržovat. To je předmětem předchozích odstavců. Další stránkou jsou ovšem smluvní odběratelko-dodavatelské vztahy mezi poskytovatelem ERP řešení a podnikem/uživatelem ERP Vision[32].

První z nich zakotvuje povinnost aktualizace software tak, aby byl v souladu s legislativou ČR a EU (podpora od výrobce), tedy s předstihem i skutečnost, že naše ERP řešení bude v souladu s GDPR. To je již dnes zakotveno v licenčních smlouvách (smlouvy o poskytování software a dalších služeb) v podobě tzv. aktualizací softwarového produktu na platnou legislativu za paušální úplatu. Veškeré tyto smlouvy budou tradičně, v případě potřeby, modifikovány a doplňovány smluvními dodatky.

Další záležitostí je smluvní ošetření případů, kdy konzultant ERP Vision[32] přistupuje k datům uživatele, což se častokrát děje pod administrátorskými právy, a tudíž v plném rozsahu, bez ohledu na to, jestli konzultant sedí fyzicky přímo u uživatele nebo přistupuje prostřednictvím nástrojů vzdálené správy. V tomto případě se my stáváme potenciálním zpracovatelem osobních údajů u našich uživatelů, což budeme muset s každým z nich formálně-právně dopředu řešit.

GDPR je přímo použitelnou a závaznou komplexní právní regulací, která bude celoevropsky účinná od 25. 5. 2018 bez ohledu na stav adaptace v českém právu. Aktuální platná a účinná česká i slovenská legislativa ochranu osobních údajů řeší a většina toho, co je předmětem GDPR už obsahuje. Na řadu aspektů je možné se připravit již dnes, ovšem řadu úskalí ukáže až samotná praxe…

Vision Praha s.r.o.
Všechromy 59
251 63 Strančice

Hodolanská 35
772 00 Olomouc

www.vision.cz
+420 585 313 130
vision@vision.cz