Soulad s GDPR

Informace o využití systému PalstatCAQ v souladu s Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 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) dále jen GDPR.

Obsah

Otázky a odpovědi

Je systém PalstatCAQ v souladu s GDPR?
Ano, nicméně je třeba upozornit, že soulad s GDPR není dán systémem PalstatCAQ, ale celkovým přístupem uživatele a způsobem nastavení a použití systému.

Je nutné aktualizovat systém PalstatCAQ na nejnovější verzi z důvodu kompatibility s GDPR?
Pokud je dobře provedeno nastavení systému a způsob jeho používání, samotná aktualizace nutná není. Aktualizace nicméně přinese nástroje pro zjednodušení správy informací v souladu s GDPR.

Je ke zpracování osobních údajů nutný souhlas subjektu, jehož data jsou zpracovávána?
Souhlas subjektu je pouze jedním z možných důvodů zpracování. Všechny uvádí GDPR v §6 čl. 1. například zpracování ze zákonných důvodů (evidence zaměstnanců), plnění smlouvy či oprávněného zájmu správce souhlas subjektu nevyžaduje. Při běžně předpokládaném užití systému PalstatCAQ bude většina osobních informací zpracovávána pravděpodobně právě z výše uvedených důvodů a nebude tak vyžadovat souhlas subjektu.

Vyžaduje GDPR šifrování dat?
Nikoliv. Veškerá opatření proti zneužití dat by měla být přiměřená a odpovídat povaze a citlivosti zpracovávaných osobních údajů a riziku jejich zneužití. Obecně lze šifrování doporučit v případě zvláštních kategorií osobních údajů, do kterých spadají například údaje o rasovém či etnickém původu, o zdravotním stavu či osobní údaje dětí. Tento druh informací není zpravidla v systému PalstatCAQ zpracováván.

Požadavky GDPR

Pro vhodné nastavení systému je třeba vycházet z požadavků GDPR. Základní postup při práci s osobními údaji by se dal shrnout takto:

1. Osobní informace
   Jaké osobní informace zpracováváte. Co jsou osobní informace je uvedeno v GDPR, zde se hodní připomenout, že se jedná o informace o konkrétních fyzických osobách. Osobní informací tedy nejsou například údaje o firmách (pokud nejde o fyzické osoby).
2. Důvod zpracování
   Ke každému druhu osobní informace je třeba znát důvod zpracování. Tím může být souhlas subjektu, ale také zákonný důvod, existující smlouva či oprávněný důvod.
3. Zásady zpracování
   Pro veškeré zpracovávané osobní informace musí být nastaveny zásady, na základě kterých s nimi pracujete. Ty by měly zahrnovat informace například o tom, kdo s těmito údaji pracuje, k čemu jsou využívány, jak dlouho jsou uchovávány a jakým způsobem jsou skartovány.
4. Záznamy o činnosti
   O činnostech, prováděných s osobními údaji, musí být vedeny záznamy. V systému PalstatCAQ k tomu slouží automatický záznam o uživateli a datu vytvoření informace a funkce Historie záznamů, která ukládá veškeré změny nastavených polí a jejich autory.
5. Zabezpečení
   Osobní údaje musí být zabezpečeny, a to s ohledem na citlivost těchto údajů, možná rizika neoprávněného přístupu k nim a jeho případných následků. Vhodné je použít přístup založený na riziku, stejně jako v případě aplikace normy ISO 9001. Šifrování informací není povinné, lze ho doporučit v případě zpracování citlivých informací (např. o zdravotním stavu apod.)

Pro popis způsobu nakládání s osobními údaji doporučujeme využít modul Procesy, který umožňuje vést dokumentaci vázanou na firemní procesy a využít přístup založený na riziku.

Nastavení systému PalstatCAQ v souladu s GDPR

Zabezpečení databáze

PalstatCAQ používá pro uložení dat databázi Microsoft SQL. Nejen v souladu s GDPR, ale z již z principů kybernetické bezpečností, je třeba zajistit minimálně:

- Umístění databáze na takovém místě, kde nebude přístupná uživatelům běžnými prostředky (tak, aby nemohlo například dojít ke zkopírování souboru databáze uživatelem).
- Zabezpečení přístupu do databáze dostatečně silným heslem.
- Naprosto nezbytné je zašifrování konfiguračního souboru systému PalstatCAQ tak, aby nemohlo dojít k neoprávněnému zjištění přihlašovacích údajů do databáze.
- Nastavení pravidelného a automatizovaného zálohování databáze na bezpečné místo. Součástí systému zálohování musí být i pravidelné ověřování jeho funkčnosti a čitelnosti záloh.

Další volitelná nastavení, v závislosti na míře citlivosti dat, mohou představovat:

- Povolení pouze šifrovaného spojení s databází
- Šifrování obsahu databáze PalstatCAQ

Zabezpečení síťového prostředí

Síťové prostředí je třeba zabezpečit proti neoprávněnému přístupu. Z pohledu systému PalstatCAQ se pak zejména v případě, že je ověřování uživatelů prováděno přes ActiveDirectory / SSO, jedná o:

- Nastavení dostatečné úrovně bezpečnosti pro ověřování uživatelů. Podle povahy a citlivosti dat to mohou být hesla odpovídající síly nebo například ověřování čipovou kartou a pinem.
- Nastavení automatického odhlašování / zamykání stanic po určité době pro zamezení neoprávněného přístupu ze stanic, kde zůstane přihlášen uživatel i při jeho nepřítomnosti.

V případě přístupu do systému PalstatCAQ z prostředí mimo lokální síť je vhodné se zaměřit na:

- Dostatečnou ochranu prostředků vzdáleného přístupu (např. Terminálový server)
- V případě potřeby zabezpečit připojení pomocí VPN

Zabezpečení přístupů do PalstatCAQ

Uživatelské přístupy do systému PalstatCAQ je třeba nastavit s ohledem na potřeby uživatelů a zároveň dostatečné zabezpečení uložených dat. Takové nastavení by mělo zahrnovat:

- Volbu odpovídajícího způsobu ověřování. Zcela jednoznačně doporučujeme využít ověřování uživatelů v ActiveDirectory z důvodu centrální správy a řady možností pro nastavení úrovně zabezpečení. Ověření formou SSO je třeba použít s rozvahou zejména s ohledem na možnost zneužití z přihlášených stanic.
- K nastavení oprávnění do jednotlivých modulů PalstatCAQ doporučujeme v maximální míře využívat skupiny uživatelů. Výhodou je nejen jednoduchost při zadávání a změnách uživatelů, ale zejména větší přehlednost.
- K ověření nastavení oprávnění do jednotlivých modulů je vhodné využít příslušný reportový dotaz.
- Uživatelům či skupinám je třeba přidělovat pouze minimální potřebná oprávnění, aby byl zajištěn jejich přístup pouze k těm informacím a úkonům, které skutečně potřebují.

Moduly PalstatCAQ

Některé moduly PalstatCAQ jsou přímo určeny pro uložení osobních informací. U těchto modulů je vhodné provést analýzu potřebnosti těchto informací a nastavení přístupu k nim.

Správa systému

Modul obsahuje číselník „Pracovníci". Jde o seznam všech zaměstnanců, který může obsahovat i bývalé či externí zaměstnance. Pro přístupu do tohoto číselníků lze v rámci modulu Správa systému nastavit samostatné oprávnění, které by mělo být přiděleno pouze velmi omezenému okruhu uživatelů.

Databáze uživatelů

Databáze uživatelů zpravidla obsahuje některé osobní údaje, jako jméno či případně email uživatele. Do databáze uživatelů by již z principu měl mít nastaven přístup pouze malý okruh uživatelů.

Výcvik

Modul obsahuje seznam všech zaměstnanců, který je shodná s e seznamem ve Správě systému a je rozšířený o některé další údaje. Protože se v tomto případě předpokládá výrazně širší zpracování osobních údajů než ve Správě systému, obsahuje modul Výcvik možnost nastavení přístupu až na úroveň jednotlivých polí. Ve funkci Chráněné informace lze nastavit, která pole jsou přístupná pouze omezenému okruhu uživatelů, kteří je potřebují ke své práci. Stejně tak lze omezit, k datům kterých zaměstnanců mají mít jednotliví uživatelé přístup.

Kontakty

Modul Kontakty je určen pro správu obchodních kontaktů (dodavatelů a zákazníků). Osobní údaje se v tomto modulu mohou vyskytovat na dvou místech. Buď jako samotný kontakt, pokud je obchodním partnerem fyzická osoba, nebo jako zaměstnanec obchodního partnera, jehož informace jsou uloženy v modulu pro účely kontaktování. V případě, že osobní údaje v modulu Kontakty existují, je třeba vhodně omezit uživatelská oprávnění tak, aby s modulem pracovali pouze uživatelé, potřebující tyto údaje ke své práci. Pokud jsou v modulu i osobní údaje dalších osob na základě souhlasu, je vhodné tento souhlas připojit do přílohy příslušného záznamu.