Informácia o podpore pre plnenie požiadaviek GDPR v programoch Fénix COMPEKO

VŠEOBECNÝ ÚVOD

Systém FENIX Compeko je súbor programov na vedenie účtovnej, personálnej a mzdovej agendy organizácií. Pozostáva zo samostatne použiteľných modulov UCT (podvojné účtovníctvo), MZD (mzdy a personalistika), FIN (financie: evidencia došlých a vyšlých faktúr a bankové operácie), MAJ (evidencia majetku), ODB (skladové hospodárstvo, odbyt a ERP) a POK (podniková pokladnica okrem ERP).
Technologicky je systém FENIX realizovaný v natívnom prostredí vývojového nástroja Microsoft Visual FoxPro, ktorý na ukladanie dát využíva iba služby súborového systému hostiteľskej platformy. Prevádzkovanie je možné na samostatnom PC, v lokálnej sieti a vo WAN sieti. Prevádzkovanie je tiež možné na Microsoft Windows platforme vo verejnom alebo privátnom cloude s bezpečným RDP prístupom priamo cez bezpečný SSL protokol alebo prostredníctvom VPN, kedy nedochádza k žiadnemu prenosu spracúvaných údajov mimo cloudu, okrem prípadov, ktoré vyžadujú relevantné zákony a predpisy (napríklad výkazy poistného, daňové hlásenia a prehľady, ...).
Naši pracovnici, ktorí prichádzajú u užívateľa do styku s osobnými údajmi, sú dostatočne znalí problematiky GDPR v takom rozsahu, aby s dátami narábali v zmysle GDPR.
Ak je pre analytické účely potrebný prenos alebo prevzatie údajov od klienta, preberajú sa spravidla údaje už anonymizovane. Po splnení účelu (analýza príčin deklarovaného problému u zákazníka, nájdenie riešenia špecifickej požiadavky, ...) sú dáta z počítača konzultanta v plnom rozsahu vymazane a nevytvárajú sa z nich žiadne ďalšie kópie.

PASÍVNA BEZPEČNOSŤ ÚDAJOV

Systém FENIX nemôže riešiť a nerieši pasívnu bezpečnosť uloženia údajov formou kryptovania alebo inou podobnou formou, nakoľko použitý vývojový prostriedok na toto nemá nástroje. Všeobecnú pasívna bezpečnosť musí riešiť správca a prevádzkovateľ hostiteľského systému (PC, lokálnej siete, cloudu, ...). Systém FENIX rieši pasívnu bezpečnosť kryptovaním iba v prípade užívateľských kont, kde na kryptovanie používa vlastný kryptovací algoritmus.

BEZPEČNOSŤ PRENOSOV

Z architektúry systému FENIX vyplýva, že nemôže riešiť otázku bezpečnosti prenosov dát. Túto oblasť musí riešiť správca a prevádzkovateľ hostiteľského prostredia.

DEFINÍCIA OSOBNÝCH ÚDAJOV

Vnútorná architektúra programov Fénix Compeko je založená na definícii pojmov (dátových elementov) v číselníku "Dátový slovník", z ktorých sú vytvárané tabuľky údajov. Definíciu osobných údajov je možné realizovať na úrovni pojmu pomocou zadania prístupu na čítanie a prístupu na zápis jednotlivých pojmov. V pojmoch definované hodnoty prístupu na čítanie a

prístupu na zápis majú priamu väzbu na bezpečnostnú úroveň pracovníka, ktorá môže byť definovaná v heslách ako "Pasívny", "Mzdár", "Osobár", "Špeciál", "Pamista", a "Správca". Prepojením prístupu na čítanie a prístupu na zápis jednotlivých pojmov s bezpečnostnou úrovňou pracovníka v heslách sa zabezpečí pre konkrétneho užívateľa sprístupnenie osobných údajov na úrovni čítania alebo zápisu. Z hľadiska GDPR je podstatná možnosť zadať pre osobné údaje retenčnú dobu. Retenčnú dobu je možné zadať na dvoch úrovniach, konkrétne na úrovni súboru (tabuľky) a na úrovni položiek (stĺpcov tabuľky – pojmov). Na úrovni súboru sa v definičnom číselníku "Súbory" zadáva retenčná doba záznamu v súbore v mesiacoch. Na úrovni položiek personálneho súboru sa zadáva jednotlivo pre vybrané osobné údaje retenčná doba poľa v súbore v mesiacoch.

MONITOROVANIE A LOGOVANIE AKTIVÍT

V systéme FENIX je možné pracovať iba po prihlásení sa platným užívateľským kontom, ktoré je vždy chránené heslom (viď časť „Prístupové práva“). V systéme sú logované všetky aktivity, ktoré menia akékoľvek dáta. Záznamy z týchto logov nie je možné užívateľsky vymazať.
V module MZD je voliteľne možné detailné logovanie zmien vybraných alebo všetkých kmeňových údajov zamestnancov s informáciou o pôvodnej a novej hodnote, s identifikáciou pracovníka, ktorý zmenu vykonal, s informáciou o dátume a čase vykonania zmeny a s identifikáciou počítača, z ktorého sa zmena vykonala. V ostatných moduloch detailné logovanie zmien nie je realizované.
Každý modul systému FENIX má vo svojich nástrojoch monitor aktuálne prebiehajúcich aktivít v celom systéme FENIX, ktorý v reálnom čase zobrazuje identifikáciu a meno pracovníka, počítač, z ktorého je prihlásený aktivitu a čas štartu danej aktivity.

PRÍSTUPOVÉ PRÁVA

Prístup do systému FENIX je chránený prepracovaným systémom hesiel k užívateľským kontám.
Detailný popis vrátane doporučeného nastavenia je v prílohe tohto materiálu.

PREHĽAD O VYKONANÝCH ZMENÁCH V DÁTACH

Na úrovni údajov v personálnom súbore, medzi ktoré patria aj osobné údaje, je možné dohľadať, ktorý užívateľ kedy a na akú hodnotu aktualizoval jednotlivé údaje. V programoch ktoré pracujú s osobnými údajmi je v skupine parametrov " Interné pre PS CPK " parameter s označením "Zapisovať zmeny kmeňových údajov ". Týmto parametrom sa určí, či sa majú zapisovať do zvláštneho súboru zmeny v kmeňových údajoch. Údaje z tohoto súboru je možné prezerať alebo vytvárať z nich rôzne tlačové zostavy podľa internej potreby. Hodnota "N" (štandard) znamená, že zmeny kmeňových údajov sa do špeciálneho súboru nezaznamenávajú. Hodnota "A" znamená, že do špeciálneho súboru sa zaznamenávajú všetky zmeny vo všetkých kmeňových údajoch. Hodnota "P" znamená, že do špeciálneho súboru sa zaznamenávajú iba zmeny vykonané v základnom kmeňovom súbore (PER). Zápis zmien kmeňových údajov do špeciálneho súboru je realizovaný v programe MZDY v častiach "Mesačné mzdové zložky", "Nároky", "Zrážky", "Aktualizácia kmeňových údajov", "Hromadná aktualizácia kmeňa" a v programe pre aktualizáciu zviazaných kmeňových súborov (súbor SPP, súbor rodinných príslušníkov...). Prezeranie špeciálneho súboru zo zmenami kmeňových dát je prístupné v časti "Aktualizácia kmeňových údajov" stlačením klávesy F3 na požadovanom údaji. Sprístupní sa "Časový vývoj kmeňového údaja", kde je možné za vybraný interval období sledovať kompletný vývoj hodnoty údaja alebo iba zmeny jeho hodnoty. V prípade číselných údajov je k dispozícii aj grafické zobrazenie vývoja hodnôt údaja. V časti "Špeciálne činnosti" sa nachádza program "LOG zmien kmeňových dát", ktorý je určený

na hromadné zobrazenie vykonaných zmien kmeňových údajov a na vytvorenie tlačových zostáv slúžiacich ako podklad k auditu zmien kmeňových údajov.
Zmeny údajov v ostatných častiach systému FENIX sa nesledujú v detailoch. V logu realizovaných činností je však záznam o tom, kto, kedy, z akého počítača vykonal operáciu, ktorou sa mohli dáta zmeniť (napr. aktualizácia KDF = Knihy Došlých Faktúr). Tieto logy sú užívateľsky nemodifikovateľné.

ANONYMIZÁCIA, PSEUDONYMIZÁCIA

V zmysle GDPR je možné evidovať a spracovávať osobné údaje iba na stanovený účel. Po pominutí účelu je nutné získané údaje zlikvidovať alebo anonymizovať. Realizácia procesu anonymizácie je založená v programoch Fénix Compeko na niekoľkých krokoch. V každom zázname, ktorým sa identifikuje doklad (faktúra, pokladničný doklad, objednávka, interný účtovný doklad...) je údaj "Dátum povinného uchovania dokladu". Tento dátum sa vypočíta individuálne pre každý druh dokladu na základe definovaných retenčných dôb údajov, ktoré sú v doklade použité (kód DPH, skupina faktúr, položky faktúr, druh pohybu, skupina objednávok, položky objednávok...). Dátum povinného uchovania dokladu (vždy najvyšší) sa spolu s údajmi o dátume použitia, podsystéme a identifikáciou dokladu zapisuje do zodpovedajúceho záznamu v číselníkoch "Obchodní partneri", "Číselník pracovníkov" alebo "Fyzické osoby". Anonymizáciu údajov v číselníkoch "Obchodní partneri", "Číselník pracovníkov" alebo "Fyzické osoby" je možné vykonať hromadne alebo jednotlivo. Hromadný spôsob, označený ako "Iniciatívne vymazanie" anonymizuje všetky záznamy s uplynutou retenčnou dobou. "Právo na zabudnutie" je spôsob určený na anonymizáciu údajov v aktívnom zázname na základe žiadosti subjektu o zabudnutie. Samotná anonymizácia predstavuje proces, kde sa do údaja s názvom subjektu zapíše výraz "Zrušené". Zároveň sa vymažú údaje ulica, PSČ, mesto, telefónne číslo, faxové číslo, mailová adresa, IČO, DIČ, IČDPH, rodné číslo, dátum poslednej aktualizácie a ID užívateľa ktorý posledný aktualizoval záznam. V prípade číselníka "Obchodní partneri" sa zrušia aj zodpovedajúce záznamy v číselníku bankových účtov a kontakty obchodného partnera.
Pri určovaní doby uchovania v podsystéme MZDY sa retenčná doba začína počítať od dátumu posledného ukončenia ľubovoľného pracovného pomeru.

NÁSTROJE NA REALIZÁCIU OPRÁVNENÝCH ŽIADOSTÍ FYZICKÝCH OSÔB

Systém FENIX má priamu procesnú podporu na realizáciu splnenia oprávnených žiadostí fyzických osôb a to:

- **Právo na prístup k osobným údajom (§21)** realizované ako súpis záznamov, v ktorých sa údaje dotknutej osoby vyskytujú vrátane informácie o retenčnej dobe každého jednotlivého záznamu alebo údaja
- **Právo na výmaz (§23)** realizované formou anonymizácie všetkých priamych výskytov údajov dotknutej fyzickej osoby, pričom program podporuje vyhľadanie všetkých výskytov v „živých“ dátach, archívnych dátach a tiež v rôznych „roztrúsených“ nesystémových kópiách dát na všetkých diskoch, ktoré sú danému procesu prístupné.
- **Právo na prenos údajov (§26)** realizované ako výpis do XML súboru, ktorý obsahuje všetky nájdené údaje dotknutej fyzickej osoby.

Tieto podporné procesy sa v každom module (podsystéme) nachádzajú vo voľbe
„Servis / G.D.P.R“

EVIDENCIE, KTORÝMI SPRACOVATEĽ A SPROSTREDKOVATEĽ

PREUKAZUJÚ PLNENIE SI POVINNOSTÍ VYPLÝVAJÚCICH Z NARIADENIA GDPR A ZÁKONA 18/2018 Z.Z. V ZNENÍ NESKORŠÍCH PREDPISOV

Systém FENIX má v sebe zabudovanú správu protokolov o iniciatívnom vymazaní a o realizácii uplatneného práva na výmaz. Retenčná doba týchto záznamov je určená systémovým parametrom a štandardne je nastavená na 4 roky od vzniku protokolu (táto doba je odvodená od štandardnej premlčacej doby v občiansko-právnom konaní). Oprávnená osoba môže z týchto protokolov pre účely preukázania plnenia si svojich povinností vytvoriť pre kontrolný orgán výpis v listinnej alebo elektronickej forme.
Systém FENIX nemá prístup a nespravuje žiadne iné údaje o procesoch a operáciách spracovateľa alebo sprostredkovateľa.

Príloha:

Doporučené nastavenia a operácie

VYBRANÉ PARAMETRE:

GDPRRQ – Podpora GDPR

Týmto parametrom sa aktivuje podpora GDPR v príslušnom podsystéme.
Odporúča sa nastaviť na hodnotu „A“

GDPRRDUD – Retenčná doba účtovných dokladov

Týmto parametrom sa určuje základná retenčná doba účtovných dokladov v mesiacoch.
Odporúča sa hodnotu tohto parametra nastaviť na 120 mesiacov.

GDPRSPD – Štandardná premlčacia doba

Týmto parametrom sa určuje základná retenčná doba na uchovávanie protokolov GDPR (napr. protokol o vymazaní údajov, protokol o exporte údajov, ...).
Odporúča sa hodnotu tohto parametra nastaviť na 48 mesiacov.

PWSECLEV – Komplexita hesiel

Týmto parametrom sa určuje požadovaná úroveň komplexity hesiel, ktoré administrátor / užívateľ prideľuje jednotlivým používateľským kontám.
Odporúča sa hodnotu tohto parametra nastaviť na **6,10,xxBxx#,3,Z090000** (detailný popis významu je v ďalšom texte)

POUŽÍVATEĽSKÉ KONTÁ – PRÍSTUPOVÉ PRÁVA

Bezpečnostná politika je v programoch Fénix Compeko zabezpečovaná pomocou definícií:

- bezpečnostnej úrovne
- komplexity hesiel
- nastavenia oprávnení pre vybrané činnosti
- možnosti zdieľania oprávnení.

V číselníku hesiel je možné nastaviť dátum, kedy skončí platnosť hesla, počet prihlásení alebo dní kedy je potrebné heslo zmeniť, požiadavku na povinnú zmenu hesla pri prvom prihlásení ako aj možnosť manuálne heslo zablokovať / odblokovať. V programoch je v skupine parametrov "EIS prostredie" parameter s označením "Komplexita hesiel". Týmto parametrom je možné nastaviť požiadavky na komplexitu zadávaných hesiel, kontrolu opakovania hesla alebo nutnosť zmeny hesla.
Pre potreby určenia bezpečnostnej úrovne systému hesiel má tento parameter niekoľko zložiek:

- Minimálna dĺžka hesla (môže sa zadať od 1 do 8) - maximálna dĺžka je vždy 8 znakov

- Počet odložených verzií hesla pre kontrolu duplicity (môže sa zadať od 00 do 20; pri počte 4 a viac sa aktivuje aj minimálna životnosť hesla 24 hodín, t.j. heslo nie je možné opätovne zmeniť skôr ako po 24 hodinách)
- požadovaná komplexita hesla: pozične predstavuje povinnosť zadať v hesle znak z príslušnej znakovej množiny. Ak sa daný znak uvedie, tak sa požaduje príslušná kontrola, ak sa na danej pozícii uvedie iný znak, kontrola sa nevykoná. V tomto údaji je možné použiť tieto znaky:
  - A - musí sa zadať aspoň jedno veľké písmeno
  - a - musí sa zadať aspoň jedno malé písmeno
  - B - musí sa zadať aspoň jedno písmeno (veľké alebo malé)
  - 1 - musí sa zadať aspoň jedna číslica
  - $ - musí sa zadať aspoň jeden špeciálny znak
  - # - musí sa zadať aspoň jedna číslica alebo jeden špeciálny znak
- Maximálny počet pokusov o zapísanie hesla. Po jeho prekročení bude konto zablokované (0-9)
- Z - pri novom konte je možné nastaviť požiadavku na zmenu hesla pri prvom prihlásení
- Počet dní pre zmenu hesla (000-999) - pri novom konte sa počet dní nastaví na tu zadanú hodnotu
- Počet prihlásení pre zmenu hesla (000-999) - pri novom konte sa počet prihlásení nastaví na tu zadanú hodnotu

Príklady:

4,05,xxB1xx
heslo v minimálnej dĺžke 4 znaky, ktoré obsahuje písmená a číslice;
test na duplicitu sa vykoná oproti posledným 5 zadaným verziám hesla;
heslo je možné zmeniť najskôr 24 hodín po poslednej zmene;
6,03,Aax1xx
heslo v minimálnej dĺžke 6 znakov, ktoré obsahuje veľké aj malé písmená a číslice;
test na duplicitu sa vykoná oproti posledným 3 zadaným verziám hesla;

***** Doporučené nastavenie *****

6,10,xxBxx#,3,Z090000

heslo v dĺžke minimálne 6 znakov, ktoré obsahuje písmená a (číslice alebo špeciálne znaky);
test na duplicitu sa vykoná oproti posledným 10 zadaným verziám hesla;
heslo je možné zmeniť najskôr 24 hodín po poslednej zmene;
pre zadanie hesla sú prípustné maximálne 3 pokusy - potom bude konto zablokované;
v novom konte sa nastaví požiadavka na zmenu hesla pri prvom prihlásení;
počet dní pre zmenu hesla sa nastaví na 90;
počet prihlásení pre zmenu hesla sa nastaví na 0

Nastavenie oprávnení sa pre konkrétneho užívateľa zadáva ako prepínač povolené / nepovolené pre jednotlivé prvky zo skupiny činností, ktoré sú definované ako spoločné operácie, spoločné číselníky, číselníky podsystému a operácie podsystému. Pre každý podsystém sú na tlačidle "Iné" prístupné definície vlastných oprávnení daného podsystému (napr. skupiny faktúr, ku ktorým má daný pracovník povolený prístup a je možné určiť, či prístup má byť aktívny alebo pasívny). Z hľadiska GDPR je to v personálnej a mzdovej agende možnosť definovať bezpečnostnú úroveň pracovníka ako "Pasívny", "Mzdár", "Osobár", "Špeciál", "Pamista", a "Správca". V heslách

definovaná bezpečnostná úroveň má priamu väzbu na definíciu prístupu na čítanie a prístupu na zápis/aktualizáciu jednotlivých pojmov (údajov), z ktorých sú vytvárané tabuľky údajov a obrazovky na vstup / zobrazenie dát.
Údaje o nastaveniach a hodnoty hesiel k jednotlivým užívateľským kontám sú ukladané v kryptovanej forme s využitím vlastného kryptovacieho algoritmu fy. Compeko.

Zdieľanie oprávnení umožní zastupovanie pracovníkov bez nutnosti zverejnenia aktuálne platných prihlasovacích hesiel. V časti "Definícia zdieľania oprávnení" je pre pracovníka s oprávnením pre aktualizáciu hesiel umožnené nadefinovať zastupovanie pracovníkov na požadovaný dátumový interval. V časti "Nastavenie" môže zastupujúci prevziať prácu v systéme so všetkými nastaveniami a oprávneniami zastupovaného. Zdieľanie oprávnení sa ukončí prihlásením zastupovaného v časti "Servis", "Identifikácia operátora".

Protokolovanie prístupov je realizované v dvoch úrovniach. Na úrovni celého systému programov Fénix Compeko je každé prihlásenie sa pracovníka do programu zaznamenané do súboru "Aktivita užívateľov", kde sú okrem označenia a mena užívateľa zapísané údaje meno podsystému, označenie počítača, popis činnosti, dátum, čas začiatku a prípadne čas ukončenia činnosti. Na úrovni jednotlivých podsystémov je konkrétna činnosť ktorá sa vykonávaná v podsystéme zaznamenaná do protokolov mesačného spracovania. V týchto súboroch sú zaznamenané údaje dátum operácie, čas začiatku a čas ukončenia činnosti, popis činnosti, označenia užívateľa, meno užívateľa a označenie počítača.

V užívateľských kontách sa odporúča nastaviť oprávnenie používať podporné operácie GDPR iba pracovníkovi, ktorý skutočne s týmito operáciami má oprávnenie a schopnosť pracovať. Ostatným pracovníkom sa odporúča túto možnosť zakázať.

PODPORNÉ OPERÁCIE

Určenie retenčnej doby a doby uchovania

Každá aktualizácia záznamov, ktoré môžu obsahovať osobné údaje, prepočíta prípadne uloží dobu uchovania daného dokladu na základe nastavených retenčných dôb častí alebo zložiek dokumentu (napr. retenčná doba danej skupiny faktúr, kódu DPH, ...). Ak sa v doklade vyskytuje referencia na záznam v číselníku obchodných partnerov, nastaví program v tomto číselníku dátum uchovania v súlade s dátumom uchovania práve aktualizovaného dokladu.

Iniciatívne vymazanie

je hromadná operácia, ktorou sa anonymizujú osobné údaje po dobe povinného uchovania. Je realizované formou anonymizácie všetkých priamych výskytov údajov dotknutej fyzickej osoby, pričom program podporuje vyhľadanie všetkých výskytov v „živých“ dátach, archívnych dátach a tiež v rôznych „roztrúsených“ nesystémových kópiách dát na všetkých diskoch, ktoré sú danému procesu prístupné. Odporúča sa túto operáciu spustiť najneskôr raz za tri roky.
Podpornú operáciu nájdeme v ľubovoľnej súčasti systému FENIX vo voľbe

Servis / G.D.P.R. / Iniciatívne vymazanie

Právo na prístup k osobným údajom (§21)

Je realizované ako súpis záznamov, v ktorých sa údaje dotknutej osoby vyskytujú vrátane informácie o retenčnej dobe každého jednotlivého záznamu alebo údaja.
Podpornú operáciu nájdeme v ľubovoľnej súčasti systému FENIX vo voľbe

Servis / G.D.P.R. / Analýza výskytu – výpis záznamov

Právo na výmaz (§23)

je realizované formou anonymizácie všetkých priamych výskytov údajov dotknutej fyzickej osoby, pričom program podporuje vyhľadanie všetkých výskytov v „živých“ dátach, archívnych dátach a tiež v rôznych „roztrúsených“ nesystémových kópiách dát na všetkých diskoch, ktoré sú danému procesu prístupné.
Podpornú operáciu nájdeme v ľubovoľnej súčasti systému FENIX vo voľbe

Servis / G.D.P.R. / Právo na zabudnutie

Právo na prenos údajov (§26)

je realizované ako výpis do XML súboru, ktorý obsahuje všetky nájdené údaje dotknutej fyzickej osoby, pričom program podporuje vyhľadanie všetkých výskytov v „živých“ dátach, archívnych dátach a tiež v rôznych „roztrúsených“ nesystémových kópiách dát na všetkých diskoch, ktoré sú danému procesu prístupné.

Podpornú operáciu nájdeme v ľubovoľnej súčasti systému FENIX vo voľbe

Servis / G.D.P.R. / Export údajov

Správa protokolov ...

Systém FENIX pri realizácii iniciatívneho vymazania, exportu dát a realizácii práva na zabudnutie vyhotoví o zrealizovaní danej operácie protokol. Tieto protokoly sú samostatnými dokladmi, ktorých retenčná doba je určená parametrom GDPRSPD (viď vyššie). Oprávnená osoba môže z týchto protokolov vyhotovovať rôzne prehľady potrebné na preukázanie splnenia si povinností vyplývajúcich z nariadenia GDPR a zo zákona 18/2018 Z.z. Záznamy po dobe uchovania sa automaticky anonymizujú.

Podpornú operáciu nájdeme v ľubovoľnej súčasti systému FENIX vo voľbe

Servis / G.D.P.R. / Správa protokolov