Bezpečnostní politika

Souhrn technických a organizačních a bezpečnostních opatření při práci s OÚ subjektů údajů (klientů) v rámci věrnostního programu Magistra program více výhod systému DAVID

LÉKÁRNA ALBA - VITAL s.r.o.
Revoluční 531
738 01 Frýdek-Místek
IČ: 268 43 391 DIČ: CZ26843391

.....

Provozovatel lékárny

14. 5. 2018

.....

Datum

Zpracování osobních údajů klientů

1.1 Principy zpracování dat

1.1.1 Oprávněnost a zákonnost

Osobní údaje klientů jsou shromažďovány a zpracovávány v souladu s platnými zákonnými normami, zejména se Zákonem č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, Zákonem č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) a Obecným nařízením o ochraně osobních údajů (General Data Protection Regulation, GDPR).

1.1.2 Omezení specifických účelů

Osobní údaje klientů jsou zpracovávány za účelem provozování věrnostního programu Magistra program Více výhod.

1.1.3 Transparentnost

Subjekt údajů (klient) je informován o tom, jak je s jeho údaji zacházeno. Osobní údaje jsou získány přímo od subjektu údajů na základě výslovného souhlasu, který uděluje klient na registračním formuláři do programu. Při shromažďování údajů je subjekt údajů informován o těchto skutečnostech:

- identita správce dat
- účel zpracování
- poučení o svých právech

1.1.4 Vymazání

Osobní údaje klientů, u kterých došlo k odvolání souhlasu či jiného zániku oprávnění ke zpracování, nejsou nadále zpracovávány.

1.1.5 Aktuálnost dat

Zpracovávané osobní údaje musí být správné, kompletní a aktuální. Nepřesné nebo nekompletní údaje mohou být opraveny/doplněny zpracovatelem či jeho zaměstnanci na základě informací, které poskytne přímo subjekt údajů.

1.1.6 Důvěrnost a zabezpečení dat

S osobními údaji klientů je zacházeno jako s důvěrnými a jsou zabezpečeny organizačními a technickými opatřeními, které zabraňují neoprávněnému přístupu, nelegálnímu zpracování nebo distribuci a stejně tak náhodné ztrátě, modifikaci nebo destrukci.

Zaměstnancům je zakázáno používat osobní údaje, které jsou jim zpřístupněny v rámci pracovního vztahu, pro soukromé nebo komerční účely, zpřístupnit je neoprávněným osobám, nebo údaje jakkoliv zpřístupnit. Zaměstnanci jsou o této skutečnosti informováni při nástupu do zaměstnání. Tato skutečnost je zakotvena do pracovní smlouvy nebo doplněna stávajícím zaměstnancům formou dodatku k pracovní smlouvě. Tento zákaz trvá i po ukončení pracovního poměru. Zaměstnanci jsou povinni se seznámit se způsoby zabezpečení počítačových systémů.

1.2 Předávání osobních údajů

Předávání osobních údajů uvnitř společnosti je povoleno pouze mezi oprávněnými osobami.
Předávání osobních údajů do třetích zemí neprobíhá.

1.3 Práva subjektů údajů

Klienti mají garantována práva, která jsou definována zákonnými normami. Jejich nárokování musí být bez zbytečného odkladu zpracováno v závislosti na povaze žádosti zodpovědným zaměstnancem lékárny nebo Pověřencem pro ochranu osobních údajů společnosti Magistra a.s (dále „DPO Magistra").

Žádost o uplatnění práva subjektem údajů musí být vyřešena bez zbytečného odkladu, nejpozději však ve lhůtě 30 dnů od přijetí požadavku.

Záznamy o nároku na uplatnění některých z práv klientů musí být neprodleně zaznamenáno do systému magistra.carecloud.cz: **Konto zákazníka/Komunikace.** Nároky jsou následně zpracovávány přímo DPO Magistra.

V případě, že žádost nelze (z jakýchkoli důvodů) zaznamenat žádost přímo v systému, zaměstnanec předá neodkladně tuto žádost DPO Magistra formou emailu na dpo@magistra.cz.

1.3.1 Právo na informace a přístup k osobním údajům

Klient může zažádat o informace, jaké osobní údaje subjektu jsou zpracovávány, jak a za jakým účelem byla data shromážděna. Zaměstnanec tuto žádost zaznamená do systému magistra.carecloud.cz, kde jí DPO Magistra vyřizuje. V případě, že žádost nelze (z jakýchkoli důvodů zaznamenat přímo v systému), zaměstnanec předá neodkladně tuto žádost DPO Magistra jiným způsobem.

1.3.2 Právo na opravu

Klient má právo na změnu, či doplnění kompletních nebo neúplných osobních údajů. Pokud jsou osobní údaje nepřesné nebo nekompletní, má subjekt údajů právo na opravu nebo doplnění. Změnu či opravu provádí zaměstnanec lékárny na základě informace od klienta přímo v systému magistra.carecloud.cz. V případě, že žádost nelze (z jakýchkoli důvodů) zaznamenat přímo v systému, zaměstnanec předá neodkladně tuto žádost DPO Magistra jiným způsobem.

1.3.3 Právo na výmaz („právo být zapomenut")

Klient může požadovat vymazání svých osobních údajů, pokud již neexistuje žádný právní důvod k jejich zpracování nebo držení. Zaměstnanec tuto žádost zaznamená do systému magistra.carecloud.cz, kde jí DPO Magistra vyřizuje. V případě, že žádost nelze (z jakýchkoli důvodů zaznamenat přímo v systému), zaměstnanec předá neodkladně tuto žádost DPO Magistra jiným způsobem.

1.3.4 Právo na omezení zpracování

Klient má právo požadovat, aby správce omezil zpracování Zaměstnanec tuto žádost zaznamená do systému magistra.carecloud.cz, kde jí DPO Magistra vyřizuje. V případě, že žádost nelze (z jakýchkoli důvodů zaznamenat přímo v systému), zaměstnanec předá neodkladně tuto žádost DPO Magistra jiným způsobem.

1.3.5 Právo na přenositelnost údajů

Klient má právo získat své osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu, a má právo předat tyto údaje jinému správci. Zaměstnanec tuto žádost zaznamená do systému magistra.carecloud.cz, kde jí DPO Magistra vyřizuje. V případě, že žádost nelze (z jakýchkoli důvodů zaznamenat přímo v systému), zaměstnanec předá neodkladně tuto žádost DPO Magistra jiným způsobem.

1.4 Kontrola bezpečnosti zpracování osobních údajů

Dodržování bezpečnostní politiky je kontrolováno pravidelně pomocí interního Auditu bezpečnosti zpracování osobních údajů dle předem definovaného plánu, min. 1x ročně. Kontrolu provádí zodpovědná osoba za bezpečnost zpracování OÚ klientů v lékárně.

1.5 Porušení bezpečnosti zpracování osobních údajů

V případě zjištění úniku osobních údajů je **zaměstnanec povinen ve lhůtě do 24 hodin informovat formou emailu** o této události Pověřence pro ochranu osobních údajů Magistra a.s. Pověřenec pro ochranu osobních údajů musí do 72 hodin od primárního zjištění únik nahlásit příslušenému správci, či orgánu.

Součástí hlášení je:

- popis porušení bezpečnosti OÚ
- kategorie OÚ
- přibližný počet dotčených zákazníků a kategorií
- popis pravděpodobných důsledků porušení
- popis navrhovaných opatření ke zmírnění možných nepříznivých dopadů.

Zabezpečení systému magistra.carecloud.cz

1.6 Oprávnění uživatelé

Do systému mají přístup pouze zaměstnanci lékárny, kteří k tomu jsou určeni, dále „oprávnění uživatelé". Jedná se o expedienty, vedoucí lékárny a majitele lékárny.

1.7 Identifikace

Oprávněné uživatele určuje majitel lékárny při zavádění provozování věrnostního programu. Majitel lékárny určuje zodpovědnou osobu za bezpečnost zpracování OÚ klientů. Oprávněné uživatele oznamuje zodpovědná osoba DPO Magistra.

Uživatelské přístupy administruje DPO Magistra, který vede seznam oprávněných uživatelů, vytváří či deaktivuje přístupové údaje. V případě, že dojde ke změně oprávněných uživatelů, je zodpovědná osoba na lékárně povinna tyto změny neodkladně nahlásit DPO Magistra, zejména v případě ukončení pracovního poměru se zaměstnancem či nástupu nového zaměstnance.

1.8 Přihlašování a ověřování

Oprávnění uživatelé se přihlašují do systému pomocí uživatelského jména a hesla. Heslo se musí skládat z nejméně osmi znaků, musí obsahovat velká písmena, malá písmena a číslice. Nesmí

obsahovat žádnou část, která by mohla být snadno spojena s oprávněným uživatelem. Přístupové údaje a hesla jsou administrovány DPO Magistra na základě aktualizace seznamu oprávněných uživatelů. Uživatelské přístupy a hesla jsou uložena takovým způsobem, aby po dobu jejich platnosti nedošlo k jejich odcizení, ztrátě či zneužití. Po 6 neúspěšných pokusech o ověření je uživatelský přístup zablokován. Uživatelské přístupy jsou deaktivovány, pokud nejsou používány po dobu nejméně 6 měsíců. Oprávnění uživatelé jsou seznámeni se zásadami práce s uživatelskými přístupy tak, aby byly pečlivě uchovány v tajnosti a nedošlo k jejich zneužití.

1.9 Kontrola přístupu

Oprávnění uživatelé mají přístup pouze k těm osobním údajům, které jsou potřeba pro výkon práce daného zaměstnavatele. Jsou rozlišeny úrovně uživatelských přístupů pro expedienty, zodpovědnou osobu a majitele lékárny.

Pro každou z výše uvedených skupin jsou vytvořeny autorizační profily, které jsou před započetím jakéhokoliv zpracování konfigurovány takovým způsobem, aby byl umožněn přístup pouze k údajům a zdrojům, jež jsou nutné k tomu, aby tito uživatelé mohli plnit své povinnosti.

Pravidelně (nejméně v kvartálních intervalech) se ověřuje, že předpoklady pro uchování příslušných autorizačních profilů stále platí. Správou autorizačních profilů je pověřen DPO Magistra.

1.10 Softwarová opatření

Pro zabraňující získání neoprávněného uživatelského přístupu do systému jsou provedena následující opatření používaného softwaru:

- nejmodernější ochranné aplikace (firewall)
- aktuální verze internetového prohlížeče

Kontrola přístupu do operačního systému i dalších systémů v lékárně (zejména pokladní systém) je nakonfigurován tak, aby byl zajištěn pouze oprávněný přístup.

1.11 Elektronické komunikační sítě

Osobní údaje nejsou distribuovány prostřednictvím elektronických komunikačních sítí.

1.12 Záložní kopie a obnovení

Lékárna neprovádí záložní kopie ani nezálohuje žádné osobní údaje klientů. Principy a postupy pro zhotovování záložních kopií a pro obnovu dat jsou smluvně ukotveny ve smlouvě se zpracovatelem osobních údajů klientů.

1.13 Seznam s přístupy

O každém přístupu do systému jsou zaznamenány (logovány) tyto údaje: uživatelské id, datum a čas přístupu, soubor nebo údaje, ke kterým se přístup uskutečnil, druh přístupu a zda to byl přístup oprávněný nebo odepřený.