GDPR v laboratořích

M. Novotný

Článek se zabývá vlivem nového evropského právního předpisu na praktické využívání informačních systémů v laboratorních provozech. Dále uvádí stav připravenosti laboratorního systému FONS Openlims společnosti Stapro s.r.o. na shodu s požadavky nařízení GDPR.

Poznámka: Zkratka GDPR označuje General Data Protection Regulation, Nařízení Evropského parlamentu a Rady (EU) č. 216/679.

NAŘÍZENÍ GDPR POSILUJE KYBERNETICKOU BEZPEČNOST ZDRAVOTNICKÝCH IS

Evropské nařízení GDPR představuje komplexní soubor pravidel na ochranu osobních údajů závazných ve všech zemích Evropského hospodářského prostoru. Nahrazuje Směrnici 95/46 EC a v České republice zákon č. 101/2000 o ochraně osobních údajů s účinnosti od 25. května 2018.

GDPR je v některých případech účelově prezentováno jako pohroma, která je odvratitelná pouze enormním úsilím a investicemi do technologií. Ve skutečnosti jde o pokračující legislativní vývoj podporující rozvoj elektronizace soukromé i veřejné sféry života občana a je jedním ze stavebních kamenů této elektronizace. Ačkoli jde o obecné nařízení zabývající se principiálně ochranou zákonných práv a svobod subjektů osobních údajů zpracovávaných v informačních systémech a svým rozsahem přesahuje hranice kybernetické bezpečnosti, v případě provozu elektronických informačních systémů poskytovatelů zdravotní péče je potřeba zaměřit pozornost primárně na tuto oblast. Cílem kybernetické bezpečnosti je, stručně řečeno, ochrana dat před zneužitím či jejich nedostupností pro oprávněného uživatele. Mezi nové požadavky, které z pohledu kybernetické bezpečnosti GDPR bezprostředně klade na zdravotnické informační systémy bez rozdílu, lze zahrnout:

- implicitní minimalizace rozsahu zpracovávaných údajů
- implicitní minimalizace doby uložení osobních údajů
- implicitní minimalizace dostupnosti údajů pro oprávněné příjemce
- bezodkladně hlásit jakýkoli únik osobních údajů dozorovému orgánu

Z těchto požadavků vyplývá nutnost revidovat funkčnost stávajících systémů právě z pohledu implicitního nastavení a odpovědět si především na následující dotazy:

1) Jaké druhy osobních údajů zpracovává daný informační systém a v souladu s jakým právním předpisem?
2) Jak je zajištěna přesnost zpracovávaných osobních údajů a jaké existují nástroje jejich validace?
3) Jak je prováděna skartace osobních údajů a jak je její provedení dokladovatelné?
4) Jakými mechanismy je zajištěna důvěrnost osobních údajů a jejich integrita v jednotlivých vrstvách informačního systému? Jak jsou tyto mechanismy (např. autentizační metody, přístupová práva, šifrovací funkce) implicitně nastaveny?
5) Jaké informace jsou obsaženy v auditních záznamech informačního systému, jak je lze publikovat a jaká je jejich vypovídající schopnost v čase (retence)?
6) Jakými mechanismy je možné aktivně upozornit správce na bezpečnostní událost detekovanou v IS?
7) Jakým způsobem bude pacientovi zpřístupněna elektronická zdravotnická dokumentace k nahlížení, či k vytvoření kopie?

Zatímco některé odpovědi budou směřovat k interní úpravě informačních systémů, jiné naopak budou naznačovat potřebu doplnění externích funkcí. Mezi horké kandidáty na externí funkce budou pravděpodobně tyto typy systémů:

- Systém pro správu digitálních identit a přístupů, který umožní centrálně spravovat životní cyklus uživatelské identity (účty, role a další atributy) v rozličných informačních systémech.
- Systém pro správu bezpečnostních záznamů (SIEM), který umožní centrální sběr auditních záznamů a dalších relevantních informací z celé IT infrastruktury včetně zdravotnických informačních systémů a jejich vzájemnou korelaci. Komerčně dostupné systémy SIEM disponují nástroji pro aktivní zasílání poplašných zpráv a dokumentaci bezpečnostních událostí.

AUDIT SYSTÉMU FONS OPENLIMS

Laboratorní informační systém FONS Openlims (FOL) společnosti STAPRO s. r. o. byl podroben internímu auditu na shodu s požadavky GDPR a dalších platných předpisů v níže uvedených oblastech:

- Zákonnost zpracování osobních údajů
- Správnost zpracování

- Omezené uložení
- Implicitní a standardní zajištění integrity a důvěrnosti
- Doložení odpovědnosti za zpracování

I. ZÁKONNOST ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Předpisy

- GDPR čl. 4 odst. 1, 5, 14 a 15
- GDPR čl. 5 odst. 1 písm. c)
- GDPR čl. 9 odst. 2 písm. h), j)
- Vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci

Druhy zpracovávaných osobních údajů

Hodnocený systém zpracovává osobní údaje o pacientech (klientech) daného zdravotnického zařízení (ZZ), o zaměstnancích ZZ – strávnících a dále o zaměstnancích ZZ pracujících ve stravovacím provozu.

Druhy zpracovávaných obecných osobních údajů pacienta:

- osobní identifikační údaje: jméno, příjmení, rodné číslo, adresa bydliště,
- kód pojišťovny.

Druhy zpracovávaných citlivých osobních údajů pacienta:

- anamnéza,
- diagnóza,
- výsledky laboratorního vyšetření.

Osobní údaje o odborném personálu laboratoře:

- osobní identifikační údaje: jméno, příjmení,
- přihlašovací jméno pro přístup do aplikace FOL.

Osobní údaje o žadatelích o vyšetření:

- osobní identifikační údaje: jméno, příjmení, titul, IČL,
- přihlašovací jméno pro přístup k aplikaci WebLIMS.

Hodnocení shody

Konstatujeme, že všechny výše uvedené druhy osobních údajů jsou zpracovávány na základě platných předpisů.

II. SPRÁVNOST ZPRACOVÁNÍ

Předpisy

- GDPR čl. 5 odst. 1 písm. d)
- GDPR čl. 16
- Zákon 372/2011 Sb., o zdravotních službách § 54 odst. 2)

Přesnost osobních údajů a zajištění práva na jejich opravu

Přesnost a správnost osobních údajů je dána spolehlivostí údajů elektronické nebo papírové žádanky o laboratorní vyšetření.

Systém umožňuje opravit osobní data pouze autorizovanému personálu.

Pojišťovna a správnost rodného čísla může být ověřována podle registru VZP.

Hodnocení shody

Konstatujeme, že je dosaženo shody s výše uvedenými předpisy.

III. OMEZENÉ ULOŽENÍ

Předpisy

- GDPR čl. 5 odst. 1 písm. e)

Skartace os. údajů

Skartace osobních údajů ve vlastním FOL není podporována.

Hodnocení shody

Konstatujeme, že v oblasti omezeného uložení není shoda s výše uvedeným předpisem.

Skartace osobních údajů pacienta v registru FOL bude doplněna do konce roku 2017.

IV. IMPLICITNÍ A STANDARDNÍ ZAJIŠTĚNÍ INTEGRITY A DŮVĚRNOSTI

Předpisy

- GDPR čl. 5 odst. 1 písm. f)
- GDPR čl. 25 odst. 2

Mechanismy

- Jde o třívrstvou databázovou aplikaci, osobní údaje jsou uloženy v databázi.
- Sekundárně jsou osobní údaje obsaženy v zálohovacím systému, který není součástí IS.
- Při souborové komunikaci s externím NIS jsou údaje uloženy v souborech síťového souborového systému (SMB nebo NFS).
- Dále se osobní údaje nacházejí na souborovém úložišti obsahujícím elektronicky podepsané dokumenty (výsledkové listy) v PDF/A formátu. Zajištění úložiště před neoprávněným přístupem je v kompetenci laboratoře. Přístup k souborům ke čtení má jen vestavěný aplikační uživatel příslušného IS.

Bezpečnostní funkce	Klientský operační systém	Databázový systém	Aplikace
Autentizace	Lokální účet, doménový účet chráněný jménem a heslem.	Aplikační a komunikační server využívají účet v databázovém systému resp. v MAD chráněný jménem a heslem.	Uživatelský účet k aplikaci chráněný jménem a heslem, resp. účet synchronizovaný z MAD.
Autorizace	Přístupová oprávnění pro uživatele klientského OS.	Nastavení role db owner pro aplikační účty.	Nastavením přístupových práv pomocí rolí (RBA) k agendám dle laboratorních provozů.
Integrita		Databázové zámky Zrcadlení SQL databáze, H-A cluster, MS Windows Cluster, zálohování a test integrity.	

Přidělení práv přístupu k agendám s osobními údaji se provádí při implementaci (po analýze provozu laboratoře) a pak následně tuto činnost provádí správce FOL.

Pohyb osobních dat:

- Osobní data do IS vstupují ve formě:
  - elektronické žádanky z NIS přenosem XML souborů dle standardu DASTA prostřednictvím síťového souborového systému (SMB/NFS) s vymezenými přístupovými právy
  - elektronické žádanky z NIS šifrovaným přenosem XML zpráv dle standardu DASTA prostřednictvím MS SQL brokeru
  - elektronické žádanky z webové aplikace WebLIMS (internetová žádanka)
  - elektronické žádanky ze systémů externích žadatelů (praktický lékař) ve formě zašifrovaných XML souborů dle standardu DASTA doručené zabezpečeným přenosovým systémem (např. MISE a.j.)
  - papírové žádanky
- Osobní data jsou z FOL předávána žadateli (lékař nebo samoplátce - fyzická osoba) o laboratorní vyšetření ve formě:
  - elektronického výsledku do žádajícího NIS přenosem XML souborů dle standardu DASTA prostřednictvím síťového souborového systému (SMB/NFS) s vymezenými přístupovými právy
  - elektronického výsledku do žádajícího NIS šifrovaným přenosem XML zpráv dle standardu DASTA prostřednictvím MS SQL brokeru
  - elektronického výsledku ve formě XML souborů dle standardu DASTA elektronicky zabezpečeným přenosovým kanálem přes Internet (systém MISE apod.)
  - on-line šifrovaného přenosu z webové aplikace WebLIMS, která je zabezpečena proti kybernetickým hrozbám na bázi metodiky OWASP
  - papírového výsledkového listu

Hodnocení shody

FOL nabízí všechny potřebné mechanismy k dosažení shody s GDPR. K porušení důvěrnosti může dojít při importu souborů s osobními údaji pacienta z externích NIS prostřednictvím síťového souborového systému (SMB/NFS), pokud tyto nejsou řádně zabezpečeny.

V. DOLOŽENÍ ODPOVĚDNOSTI ZA ZPRACOVÁNÍ

Předpisy

- GDPR čl. 5 odst. 2

Auditní stopa

Tabulka níže zachycuje způsob záznamu a typ zaznamenávaných událostí.

Vrstva	Nástroj	Druh záznamu	Přístup k záznamům	Retence
Aplikace	Databázová tabulka	Evidence (logování) všech změn v db FOL formou interních deníků. Jsou uchovávány celé tiskové sestavy Přístup do WebLIMS zaznamenáván včetně evidence pasivních přístupů k výsledkům.	Administrátor FOL	Nastavitelná
Databáze	DB log	Přihlášení aplikačního účtu	Administrátor IT	Nastavitelná
OS	Event Log	Přihlášený uživatel v roli správce	Administrátor IT	Nastavitelná

Všichni oprávnění uživatelé musí mít implicitně přístup ke všem osobním údajům pacientů vyskytujícím se v daném laboratorním provozu, proto jednotlivé přístupy nejsou zaznamenávány.

Hodnocení shody

FOL nabízí všechny potřebné mechanismy k dosažení shody s GDPR.

ZÁVĚR

Z výše uvedeného vyplývá, že lépe jsou na shodu s požadavky GDPR připravena ta zdravotnická zařízení, která mají zavedený systém řízení informační bezpečnosti dle zákona o kybernetické bezpečnosti či dokonce disponují certifikací dle ČSN ISO/IEC 27001:2013. Je třeba počítat s tím, že jednou zavedený systém správy informační bezpečnosti bude nutné natrvalo udržovat aktuální a že bude natrvalo konzumovat provozní náklady spíše se zvyšující se tendencí. Taková je daň, kterou je potřeba zaplatit za komfort, který nám informační společnost poskytuje. Společnost Stapro tuto skutečnost vnímá a působí svými systémy proti tomuto trendu tak, že je vybavuje potřebnými mechanismy, aniž by tím zvyšovala pořizovací cenu či náročnost instalace svých produktů.