Uchovávání obrazové dokumentace v souladu s GDPR

Petr SIBLÍK

petr.siblik@i.cz

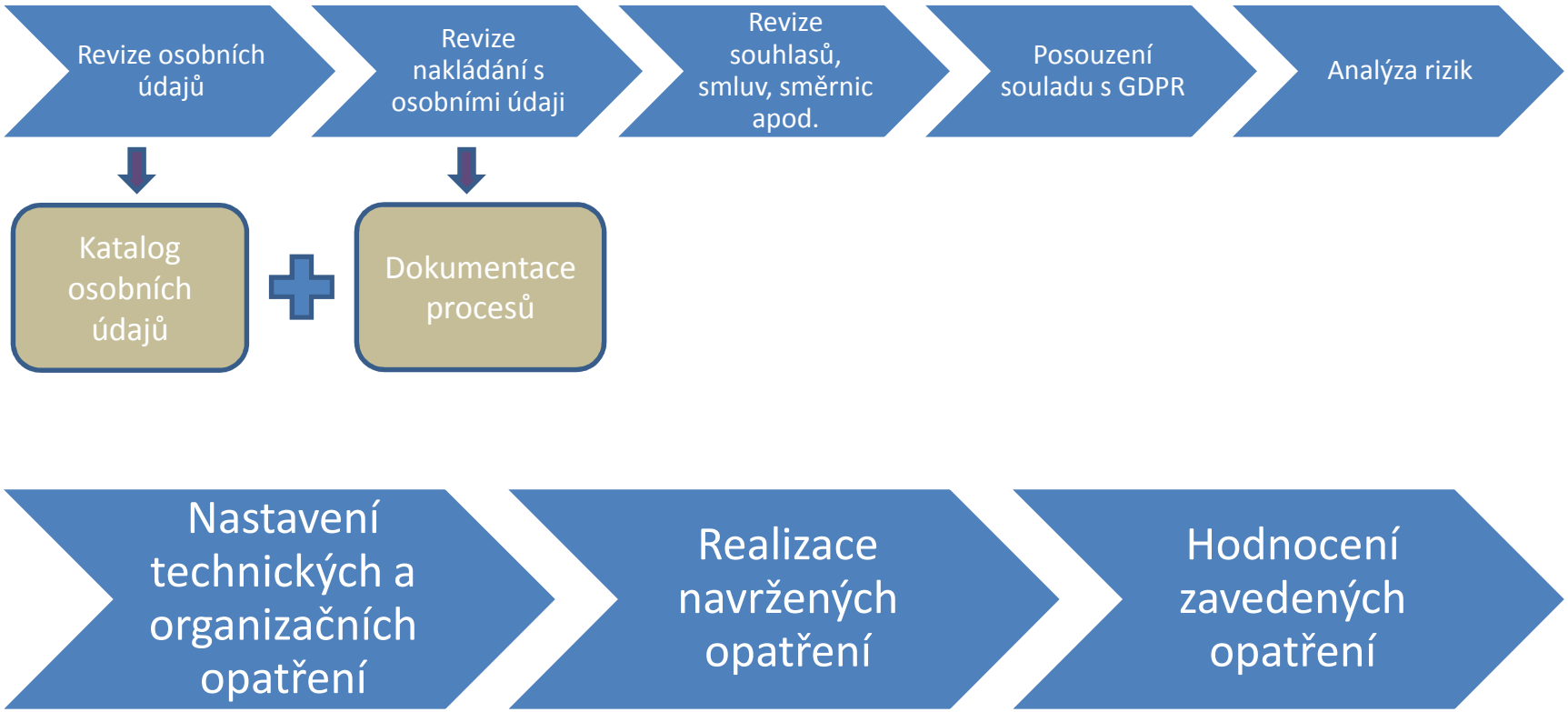
ICZ a.s.


25. května
GDPR
Noc kostelů

Rekapitulace

- ✓ Co je GDPR
- ✓ Oblast působnosti
- ✓ Osobní údaje
- ✓ Zpracování osobních údajů
- ✓ Citlivé osobní údaje
- ✓ Výjimky pro zpracování citlivých údajů
- ✓ Práva subjektů údajů
- ✓ Povinnosti správců/zpracovatelů
- ✓ Zavádění technických a organizačních opatření
- ✓ Zabezpečení zpracování
- ✓ Vedení záznamů o zpracování
- ✓ Hlášení případů porušení zabezpečení osobních údajů
- ✓ Posouzení vlivu zpracování na ochranu osobních údajů
- ✓ Předchozí konzultace
- ✓ Předávání do třetích zemí
- ✓ Pověřenec pro ochranu osobních údajů
- ✓ Úkoly pověřence
- ✓ Kodexy chování
- ✓ Náplň kodexů chování
- ✓ Monitorování dodržování kodexu chování
- ✓ Osvědčení o ochraně údajů
- ✓ Správní sankce
- ✓ Podmínky uložení pokuty
- ✓ Dozorový orgán
- ✓ Očekávané zpřesnění v souvislosti s GDPR
- ✓ …
- ? **Implementace GDPR**

Postup implementace GDPR



Oblast působnosti GDPR

Vztahuje se na:

- **S-správce** (poskytovatel zdravotní služby)
- **Z-zpracovatele** (provozovatel IS; dodavatel IS, pokud v rámci služeb provádí zpracování údajů)

Písemná smlouva nebo jiný právní akt mezi S a Z

Dopady právního vztahu

- …
- Služby podpory, při kterých dochází ke zpracování údajů, lze poskytovat jen v rámci právního vztahu se správcem
- Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce
- …

Výjimky pro zpracování citlivých údajů

- …
- pro účely archivace ve veřejném zájmu, **vědeckého** a historického výzkumu a statistické účely
- …

- Anonymizace nebo pseudonymizace dat
- Oddělené uložení od báze pacientských dat

Řešení ICZ pro podporu eZD

Obrazová dokumentace

- Zobrazování a popis ⇒ DicompassWeb
- Dlouhodobé ukládání ⇒ FlexServer
- Výměna ⇒ ePACS ComNode

Textová dokumentace

- Zobrazování a popis ⇒ AMIS*HD
- Dlouhodobé ukládání ⇒ Archív ZD
- Výměna ⇒ ISAC

Identifikace, autentizace a autorizace

- Použití metod identifikace a autentizace pro uživatele i komponenty nabízejících odpovídající záruky (využití externí databáze uživatelů – LDAP/AD/Kerberos, SAML, …)
- Správa uživatelských účtů v IS
- Bezpečné ukládání hesel a jiných autentizačních prvků
- Řízení přístupů k funkcionalitě a datům na základě rolí

Ochrana údajů před prozrazením

- Šifrování přenosů
- Šifrování uložených dat
- Správa klíčů použitých pro šifrování
- Anonymizace

Ochrana údajů před změnou

- Používání kontrolních kódů
- Podepisování elektronickým podpisem

Auditní logování

Možnosti provozního a auditního logování:

- globální
- čtení
- na úrovni jednotlivých obrazových dat
- detailu události (včetně dat)
- uživatelský přístup vs. napojení na SIEM

Příklad údajů auditního záznamu:

Detail události:

ID události = {86478}
Typ události = {UPDATE_PATIENT}
Datum a čas = {2018-01-17 13:52:48}

Původce události:

Entita = {User}
Jméno uživatele = {admin}
ID uživatele = {Administrator}
Lokální uživatel = {true}
Role = {audit, admin, }
Skupiny = {}

Text události:

UID={1.3.6.1.4.1.20744.3.1.2.2.33.1511383164756.85830}

Zálohování a zajištění dostupnosti

Řešení dostupnosti a ochrany proti ztrátě dat řeší i ochranu osobních údajů:

- Krátkodobý (STA) a dlouhodobý archív (LTA)
- Centrální archív
- Architektura Master – Slave v řešení HA-DR

Skartace dokumentace dle zákona

Propagace skartace do zdrojových IS

Uplatnění práv subjektu údajů

- Informování o zpracovávaných údajích
- Oprava údajů
- Výmaz údajů
- Omezení zpracování
- Oznamovací povinnost
- Přenositelnost údajů

www.i.cz