Implementace GDPR ve zdravotnictví

legislativní pohled
praktické implementační kroky

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Konference Moderní veřejná správa 24.5.2018

Mgr. JUDr. Vladimíra Těšitelová

statutární zástupce ředitele ÚZIS ČR

ÚZIS Ústav zdravotnických informací a statistiky ČR
Institute of Health Information and Statistics of the Czech Republic

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

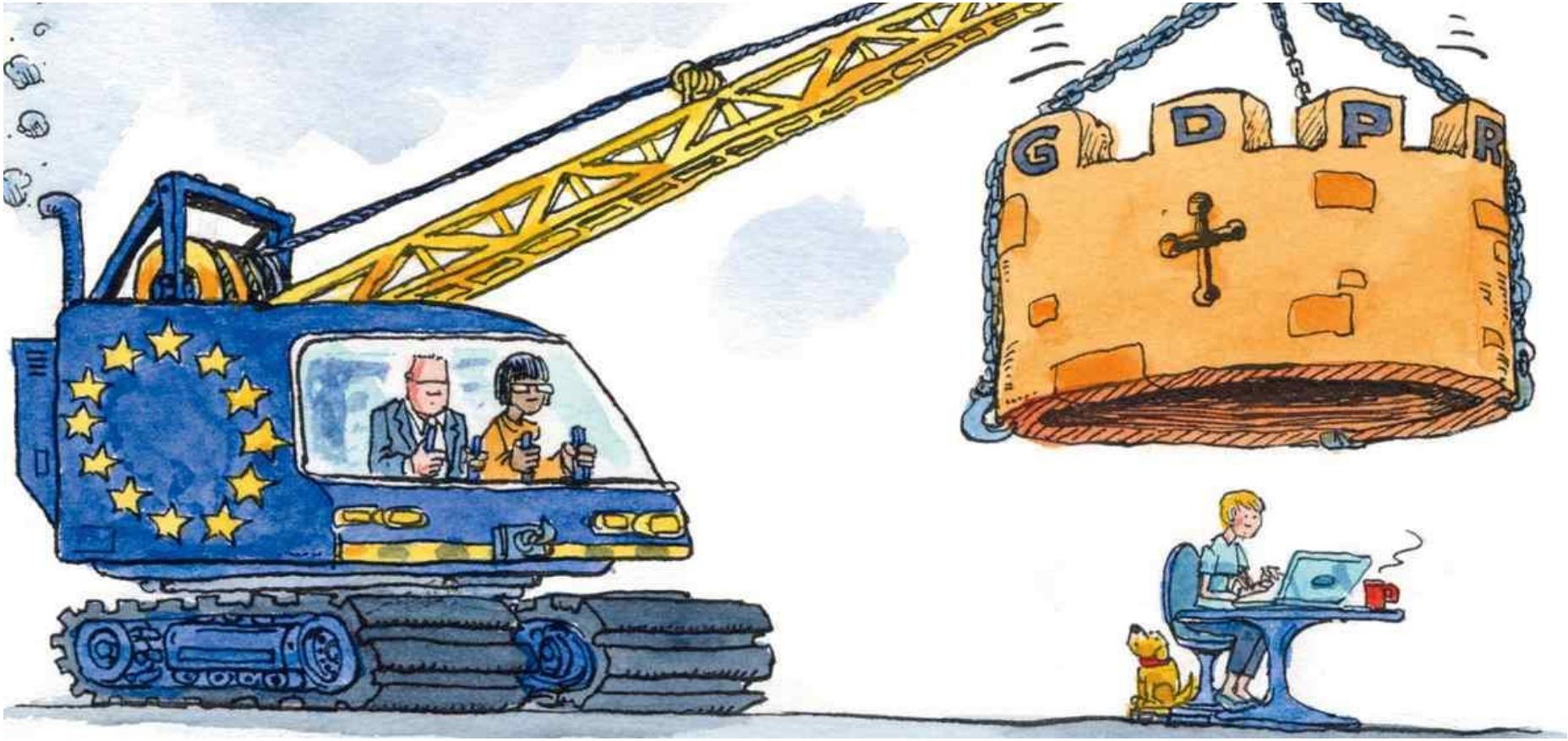
Obsah a cíle sdělení

1. Aktivity MZ ČR v oblasti implementace GDPR
2. Jaké změny přináší GDPR do zdravotnictví
3. Zpracování metodologie implementace GDPR pro přímo řízené organizace MZ ČR a ambulance, vč. zpracování konkrétních šablon
4. Některé konkrétní otázky týkající se některých konkrétních práv subjektu údajů a povinnosti správců/zpracovatelů
5. Desatero k implementaci - praktické kroky
6. Zkušenosti ÚZIS ČR

ÚZIS ČR

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Jak je GDPR vnímána ve společnosti



ÚZIS ČR

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Aktivity Ministerstva zdravotnictví ČR

- analýza resortní právní úpravy ČR ve vazbě na ustanovení GDPR umožňující výjimky právní úpravou členského státu, vč. výjimek pro účely vědeckého a historického výzkumu, pro statistické účely i pro účely archivace ve veřejném zájmu,
- zpracování metodologie implementace GDPR pro přímo řízené organizace MZ ČR a ambulance, vč. zpracování konkrétních šablon ve spolupráci s Ústavem zdravotnických informací a statistiky ČR (ÚZIS ČR),
- pravidelné semináře pro zástupce poskytovatelů zdravotních služeb,
- kurz pro pověřence pro ochranu osobních údajů,
- zavedení adresy: gdrp@mzcr.cz pro dotazy k GDPR……etc.

ÚZIS ČR

Aktivity Ministerstva zdravotnictví ČR

ÚZIS ČR

- je organizační složkou státu, která je MZ ČR zřízena k plnění úkolů MZ ČR v oblasti zajištění Národního zdravotnického informačního systému (NZIS) podle zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) ve znění pozdějších předpisů, a zákona č. 89/1995 Sb., o státní statistické službě, ve znění pozdějších předpisů,
- je správcem NZIS, provozuje 46 registrů.

ÚZIS ČR

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Jaké změny přináší GDPR do zdravotnictví

Analýza právní úpravy ČR shledala, že :

- **resort zdravotnictví je resortem z pohledu ochrany osobních údajů, resp. zvláštních kategorií osobních údajů (zdravotní stav) již v současné době resortem přísně regulovaným,**
- **bylo shledáno, že stávající nastavená regulace platnými právními předpisy je obecně dostatečná, zejména s ohledem na :**

ÚZIS ČR

Jaké změny přináší GDPR do zdravotnictví

- zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) ve znění pozdějších předpisů

Konkrétní příklad:

- ☑ Pro vedení zdravotnické dokumentace jsou to ustanovení § 53-69 o zdravotnické dokumentaci a navazující prováděcí vyhláška MZ ČR č. 98/2012 Sb., o zdravotnické dokumentaci.
- ☑ Pro správu NZIS a povinnosti ÚZIS ČR jako správce jsou to ustanovení § 70-78 a navazující prováděcí vyhlášky MZ ČR č. 373/2016 Sb., o předávání údajů do Národního zdravotnického informačního systému.

Jaké změny přináší GDPR do zdravotnictví

- zákon č. 373/2011 Sb., o specifických zdravotních službách ve znění pozdějších předpisů,

  Konkrétní právní úprava práv a povinnosti pacientů a poskytovatelů zdravotních služeb a práva a povinnosti dalších právnických a fyzických osob v souvislosti s poskytováním specifických zdravotních služeb, zahrnující i zpracování osobních údajů, vč. jejich předávání dalším příjemcům,

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Jaké změny přináší GDPR do zdravotnictví

- zákon č. 374/2011 Sb., o zdravotnické záchranné službě ve znění pozdějších předpisů

  Konkrétní právní úprava práv a povinností poskytovatelů zdravotnické záchranné služby, řešení krizových a mimořádných událostí zahrnující i zpracování osobních údajů.

- zákon č. 378/2007 Sb., o léčivech, ve znění pozdějších předpisů

  Konkrétní příklad:

  Pravomoci správních orgánů v oblasti humánních léčiv či veterinárních léčiv, vč. sběru a zpracování osobních údajů, centrální úložiště receptů …..atd.

ÚZIS ČR

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Jaké změny přináší GDPR do zdravotnictví

- změny zaváděné GDPR ve zdravotnictví jsou, při respektování stávající právní úpravy stanovené zejména právními předpisy pro resort zdravotnictví, změnami minimálními či zpřesňujícími,

GDPR není revolucí je evolučním procesem příležitostí

ÚZIS ČR

Jaké změny přináší GDPR do zdravotnictví

- velkým přínosem implementace GDPR je zejména:
  - inventarizace či zpřehlednění všech zpracovávání osobních údajů (nejen ve zdravotnické dokumentaci) a jejich porovnání se základními principy GDPR (zejména z pohledu zákonnosti, účelu i minimalizace),
  - opětovné uvědomění si, co vše jest osobním údajem,
  - zopakování či připomenutí si ochrany osobních údajů a zásad jejich zpracování.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Metodologie implementace GDPR pro přímo řízené organizace MZ ČR

Autorský kolektiv:
Mgr. JUDr. Vladimíra Těšitelová, zástupce ředitele ÚZIS ČR
JUDr. Radek Policar, náměstek ministra zdravotnictví
Ing. Milan Blaha, Ph.D., vedoucí odboru IT ÚZIS ČR
RNDr. Daniel Klimeš, Ph.D., vedoucí datového centra ÚZIS ČR
doc. RNDr. Ladislav Dušek, Ph.D., ředitel ÚZIS ČR

http://www.mzcr.cz/Legislativa/dokumenty/metodika-implementace-gdpr_14864_3805_11.html

Zdroj: ÚZIS ČR

Metodologie implementace GDPR pro přímo řízené organizace MZ ČR

- jedná se o doporučující materiál zpracovaný pro přímo řízené organizace MZ ČR, zejména pro velké celky (např. nemocnice),
- materiál byl zpracován ve verzi 1.1 a bude průběžně aktualizován (cca v roční frekvenci či dle potřeby), mimo jiné i návazně na doporučující stanoviska dozorového úřadu a skupiny WP 29,
- konzultováno:
  - Úřad pro ochranu osobních údajů
  - MV ČR, odbor legislativy a koordinace předpisů.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Metodologie implementace GDPR pro přímo řízené organizace MZ ČR

Metodika

10 kapitol

Od obecného uvedení do problematiky GDPR, výjimky pro resort zdravotnictví až po konkrétní implementační kroky.

8 příloh

Ukázky praktických dokumentů či metodických návodů na zpracování, vč. checklistu.

Formát A 5
10 kapitol
8 příloh
114 stran

Poznámka

Obě části zahrnují popisy, definice, názorné tabulky s popisem regulace a konkrétním dopadem pro správce/zpracovatele osobních údajů

ÚZIS

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Metodologie implementace GDPR pro ambulance

Autorský kolektiv:
Mgr. JUDr. Vladimíra Těšitelová, zástupce ředitele ÚZIS ČR
JUDr. Radek Policar, náměstek ministra zdravotnictví
doc. RNDr. Ladislav Dušek, Ph.D., ředitel ÚZIS ČR

http://www.mzcr.cz/Legislativa/dokumenty/metodika-implementace-gdpr-v-ambulantni-sfere_14867_3805_11.html

Zdroj: ÚZIS ČR

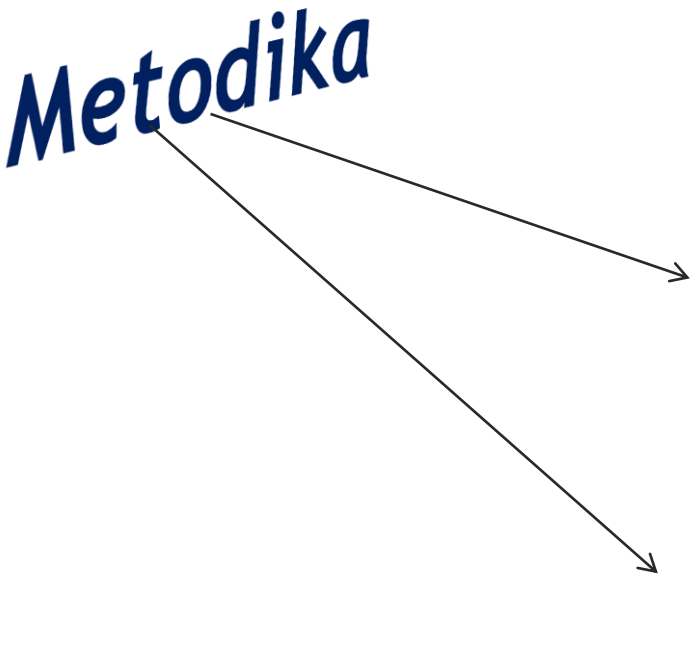
Metodologie implementace GDPR pro ambulance

- jedná se o doporučující materiál zpracovaný pro ambulance, zejména pro malé provozy (např. ambulance jeden lékař a sestra),
- materiál byl zpracován ve verzi 1, prošel odbornou oponenturou a vdána verze 2 a bude průběžně aktualizován (dle potřeby), mimo jiné i návazně na doporučující stanoviska dozorového úřadu a skupiny WP 29,
- konzultováno:
  - Úřad pro ochranu osobních údajů
  - MV ČR, odbor legislativy a koordinace předpisů.
- cílem je přispět k lepší orientaci poskytovatelů ambulantních zdravotních služeb v dané problematice.

ÚZIS ČR

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Metodologie implementace GDPR pro přímo řízené organizace MZ ČR



Formát A 5
7 kapitol
8 příloh
106 stran

Od obecného uvedení do problematiky GDPR, výjimky pro resort zdravotnictví až po konkrétní implementační kroky.

Ukázky praktických dokumentů či metodických návodů na zpracování, vč. Otázek a odpovědí

Poznámka

Obě části zahrnují popisy, definice, názorné tabulky s popisem regulace a konkrétním dopadem pro správce/zpracovatele osobních údajů

ÚZIS

Přílohy - příklady

Katalog osobních údajů Katalog operací

- obsahuje základní rozčlenění v celkové tabulce a
- následně pak popis jednotlivých jejích součástí ve sloupcích s možností jejich kategorizace a číselníkového vyjádření.,
- pro praktické užití je možné tabulku zpracovat ve formátu MS Excel s přednastavenými možnostmi vyplnění jednotlivých polí či zpracovat speciálního SW, který by uvedené parametry zautomatizoval.

Datový zdroj	Osobní údaj	Subjekt osobních údajů	Kategorie osobních údajů	Právní titul	Získáno od subjektu údajů či nikoliv	Účel	Operace	Proces zdokumentován	Odpovědnost

Přílohy - příklady Číselníky

Číslo operace	Název operace	Obsah operace
1	SHROMÁŽDĚNÍ	SBĚR OSOBNÍCH ÚDAJŮ
2	ZAZNAMENÁNÍ	UMÍSTĚNÍ OSOBNÍCH ÚDAJŮ V INFORMAČNÍCH ČI JINÝCH SYSTÉMECH
3	KONTROLA	POROVNÁNÍ JIŽ SHROMÁŽDĚNÝCH NEBO ZAZNAMENANÝCH ÚDAJŮ S ÚČELEM
4	STRUKTUROVÁNÍ	TRANSFORMACE OSOBNÍCH ÚDAJŮ
5	ULOŽENÍ	UKLÁDÁNÍ OSOBNÍCH ÚDAJŮ DO DATABÁZÍ
6	VALIDACE	KOREKCE SYSTÉMOVÝCH CHYB A ZKRESLENÍ
7	VYHLEDÁNÍ	APLIKAČNÍ A ANALYTICKÁ PRÁCE S OSOBNÍMI ÚDAJI
8	NAHLÉDNUTÍ	APLIKAČNÍ A ANALYTICKÁ PRÁCE S OSOBNÍMI ÚDAJI
9	POUŽITÍ	APLIKAČNÍ A ANALYTICKÁ PRÁCE S OSOBNÍMI ÚDAJI
10	ZPŘÍSTUPNĚNÍ PŘENOSEM	PŘEDÁNÍ OSOBNÍCH ÚDAJŮ
11	ŠÍŘENÍ NEBO JAKÉKOLIV JINÉ ZPŘÍSTUPNĚNÍ	ZPŘÍSTUPNĚNÍ ČI PUBLIKACE OSOBNÍCH ÚDAJŮ (ZPRAVIDLA AGREGACE)
12	SEŘAZENÍ ČI ZKOMBINOVÁNÍ	ANALYTICKÁ PRÁCE S OSOBNÍMI ÚDAJI
13	OMEZENÍ	OZNAČENÍ ULOŽENÝCH OSOBNÍCH ÚDAJŮ ZA ÚČELEM OMEZENÍ JEJICH ZPRACOVÁNÍ V BUDOUCNU
14	VÝMAZ NEBO ZNIČENÍ	
15	ZPŘÍSTUPNĚNÍ DALŠÍMU ZPRACOVATELI	ZPŘÍSTUPNĚN NA ZÁKLADĚ SMLOUVY O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ
16	ANONYMIZACE	TAKOVÁ ZMĚNA OSOBNÍCH ÚDAJŮ, V JEJÍMŽ DŮSLEDKU JE PŘIŘAZENÍ OSOBNÍCH ÚDAJŮ URČITÉ FYZICKÉ OSOBĚ NEMOŽNÉ NEBO MOŽNÉ POUZE ZA NEPŘIMĚŘENÉHO VYNALOŽENÍ ČASU, NÁKLADŮ A PRACOVNÍHO ÚSILÍ.
17	PSEUDONYMIZACE	ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ TAK, ŽE JIŽ NEMOHOU BÝT PŘIŘAZENY KONKRÉTNÍMU SUBJEKTU ÚDAJŮ BEZ POUŽITÍ DODATEČNÝCH INFORMACÍ, POKUD JSOU TYTO DODATEČNÉ INFORMACE UCHOVÁVÁNY ODDĚLENĚ A VZTAHUJÍ SE NA NĚ TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, ABY BYLO ZAJIŠTĚNO, ŽE NEBUDOU PŘIŘAZENY IDENTIFIKOVANÉ ČI IDENTIFIKOVATELNÉ FYZICKÉ OSOBĚ

Přílohy - příklady

Smlouva o zpracování osobních údajů (výňatek)

Článek GDPR	Povinnost správce/zpracovatele	Dopad do smlouvy
čl. 28 odst. 9	Požadavek na písemnou formu, vč. elektronické formy.	Smlouva musí mít písemnou formu. Zásadně a bezvýjimečně.
čl. 28 odst. 1	Správce může jako zpracovatele zapojit pouze takového zpracovatele, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.	Je nutné explicitní prohlášení zpracovatele, že zaručí zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.
čl. 28 odst. 2, věta první	Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce.	V případě, že je předpoklad „řetězení zpracovatelů“, je nutné explicitně uvést do ustanovení smlouvy ve variantě konkrétního nebo obecného písemného povolení ze strany správce.
čl. 28 odst. 2, věta druhá	V případě obecného písemného povolení zpracovatel správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak správci příležitost vyslovit vůči těmto změnám námitky.	Je-li ve smlouvě uvedeno obecné povolení ze strany správce, že je umožněno „řetězení zpracovatelů“ je nutné zakotvit ve smlouvě proceduru pro přijetí nových zpracovatelů nebo jejich nahrazení a pro reakci správce.
čl. 28 odst. 3, věta první	Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie	V současnosti dle § 6 ZOOÚ. Smlouva musí obsahovat taxativně uvedené náležitosti: ➢ závazky zpracovatele vůči správci, ➢ předmět a doba trvání zpracování, ➢ povaha a účel zpracování, ➢ typ osobních údajů,

Některé konkrétní otázky

- **Otázka č. 1: Týká se vůbec GDPR primární a specializované ambulantní péče?**

Odpověď:

Ano, týká, protože zpracovávají osobní údaje, včetně zvláštní kategorie osobních údajů podle platných právních předpisů resortu zdravotnictví. Nicméně je třeba k implementaci přistupovat přiměřeně a zejména u malých ambulancí by implementace GDPR neměla znamenat významnou organizační či administrativní zátěž.

Některé konkrétní otázky

- **Otázka č. 14: Musí se pro vedení primární zdravotnické dokumentace vést informovaný souhlas pacienta?**

Odpověď:

Ne, jedná se o plnění právní povinnosti pro lékaře, která vyplývá z právních předpisů ČR a GDPR umožňuje tuto úpravu využít.

Některé konkrétní otázky

- **Otázka č. 13: Praktický lékař sdílí dokumentaci a výsledky s jinými lékaři, nemocnicemi – je tato komunikace a předávání informací o jím vedených pacientech nadále možná bez zvláštních smluv? Nebo bude nutné uzavírat nějaké smlouvy se všemi poskytovateli, se kterými informace sdílí?**

Odpověď:

Smlouva není potřeba za předpokladu, že se jedná o zajištění návaznosti dalších zdravotních nebo sociálních služeb pro pacienty. To platí za předpokladu, že budou dodrženy ostatní povinnosti dle GDPR – např. zabezpečená forma předání, kontrola přístupu k citlivým a osobním údajům, apod. V jiných situacích smlouva zapotřebí je, například pokud se jedná o klinickou studii, zpracování dat nesouvisející se zajištěním zdravotních nebo sociálních služeb apod.

ÚZIS ČR

Desatero k implementaci GDPR - praktické kroky

(výňatek)

ODPOVĚĎ NA OTÁZKY CO MÁM MIT PŘIPRAVENO:

1. katalog osobních údajů - INVENTURA CO MÁM, MŮŽU TO MÍT etc.;
2. katalog operací - může být pokračováním katalogu osobních údajů a ZÁKLADEM PRO PROKÁZÁNÍ SOULADU S GDPR;
3. analýza připravenosti na GDPR a prokázání souladu s GDPR - zpracování POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ (není vždy nutné), ANALÝZY RIZIK, ZÁZNAMŮ O ČINNOSTECH ZPRACOVÁNÍ - zní to složitě, ale v podstatě se může jednat o excelovskou tabulku ;
4. jasně zavedenou agendu přístupů k osobním údajům (tím se plní i technicko-organizační opatření);
5. technická a organizační opatření - NEZAPOMENOUT NA ÚPLNĚ OBYČEJNÁ - např. zamykání dveří etc.

ÚZIS ČR

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Desatero k implementaci GDPR - praktické kroky

JEDNÁ SE O DOPORUČENÍ (GDPR=odpovědnost správce)

ODPOVĚĎ NA OTÁZKY CO MÁM MIT PŘIPRAVENO:

5. proškolení osob;
6. řádně sepsaná smlouva o zpracování osobních údajů se zpracovateli, mám-li je;
7. připravená informace o zpracování osobních údajů - dle parametrů GDPR a pomůckou může být KATALOG OSOBNÍCH ÚDAJŮ, OPERACÍ I ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ,
8. event. připravený souhlas se zpracováním osobních údajů - tam, kam nedosáhne právní úprava, výkon pravomoci;
9. pravidelnou kontrolu - je nutné kontrolovat pravidelně, jako např. BOZP či přezkoušení řidiče referenčního vozidla etc.
10. pravidelnou aktualizaci - v momentě, kdy je zjištěno vybočení z nastavených pravidel - okamžitě musí následovat změna - byť obyčejná - např. při příjmu nového zaměstnance či u jeho uko[illegible] hlášení dozorovému úřadu či subjektu údajů apod.

ÚZIS

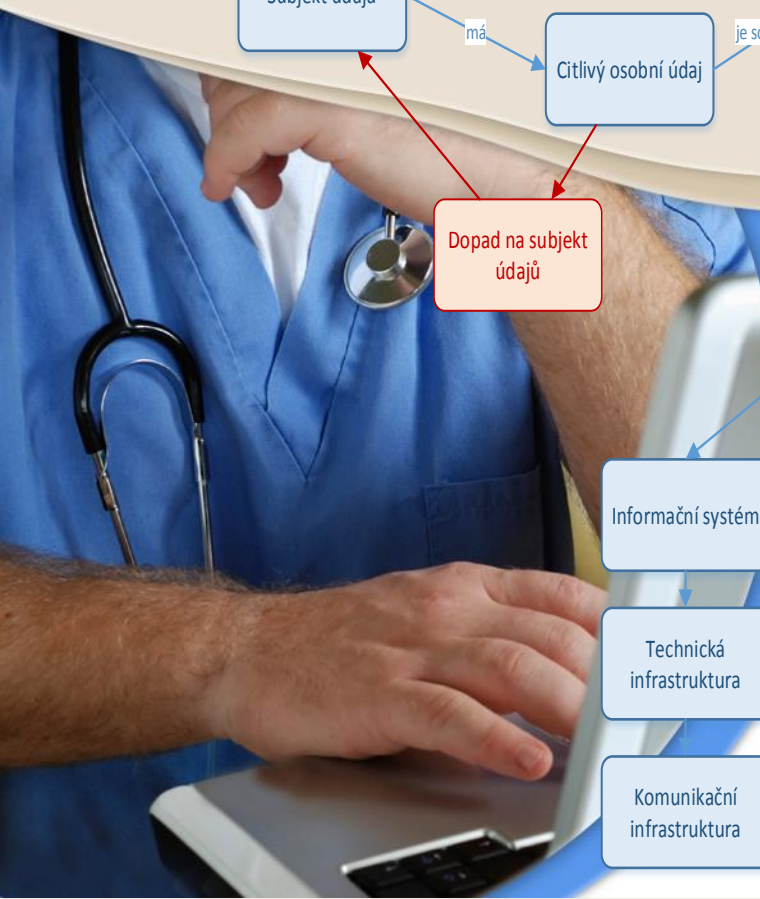
Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Zkušenosti ÚZIS ČR

- ☑ jmenován pověřenec pro ochranu osobních údajů;
- ☑ již v průběhu legislativního procesu novely zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) realizovaný zákonem č. 147/2016 Sb., i jeho prováděcí vyhlášky č. 373/2016 Sb., o předávaní údajů do NZIS zohledňován dopad na ochranu osobních údajů;
- ☑ katalog osobních údajů většinou stanovený právními předpisy;
- ☑ in-house vývoj nových komponent NZIS dle moderních pravidel eGov;
- ☑ příprava věcného záměru o NZIS;
- ☑ rekonstrukce celého NZIS (vč. starých komponent) dle moderních pravidel eGov – pseudonymizace dle pravidel GDPR.....etc.

ÚZIS ČR

Koncepční schéma řízení GDPR ÚZIS



Dopad na subjekt údajů

Konkrétní kolekce osobních údajů v určitém systému zpracování informací (IS, kartotéka, …), zpracovávaná za specifickým účelem

Osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný

Expirace / spouštěcí událost

Osobní údaj

Subjekt údajů

má

má

Citlivý osobní údaj

je součástí

je součástí

Katalog OÚ

je zpracovávána pro dosažení

Účel zpracování

je zpracovávána v rámci

Zákonný důvod zpracování

Dopad na subjekt údajů

Systém zpracování informací

Zpracování je zákonné, pokud
a) subjekt údajů udělil souhlas
b) zpracování je nezbytné pro splnění smlouvy,
c) zpracování je nezbytné pro splnění právní povinnosti
d) zpracování je nezbytné pro ochranu životně důležitých zájmů
e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci
f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany

využívá

využívá

využívá

Informační systém

Ostatní prostředky zpracování

Non-IT prostředek zpracování

Technická infrastruktura

Riziko zpracování

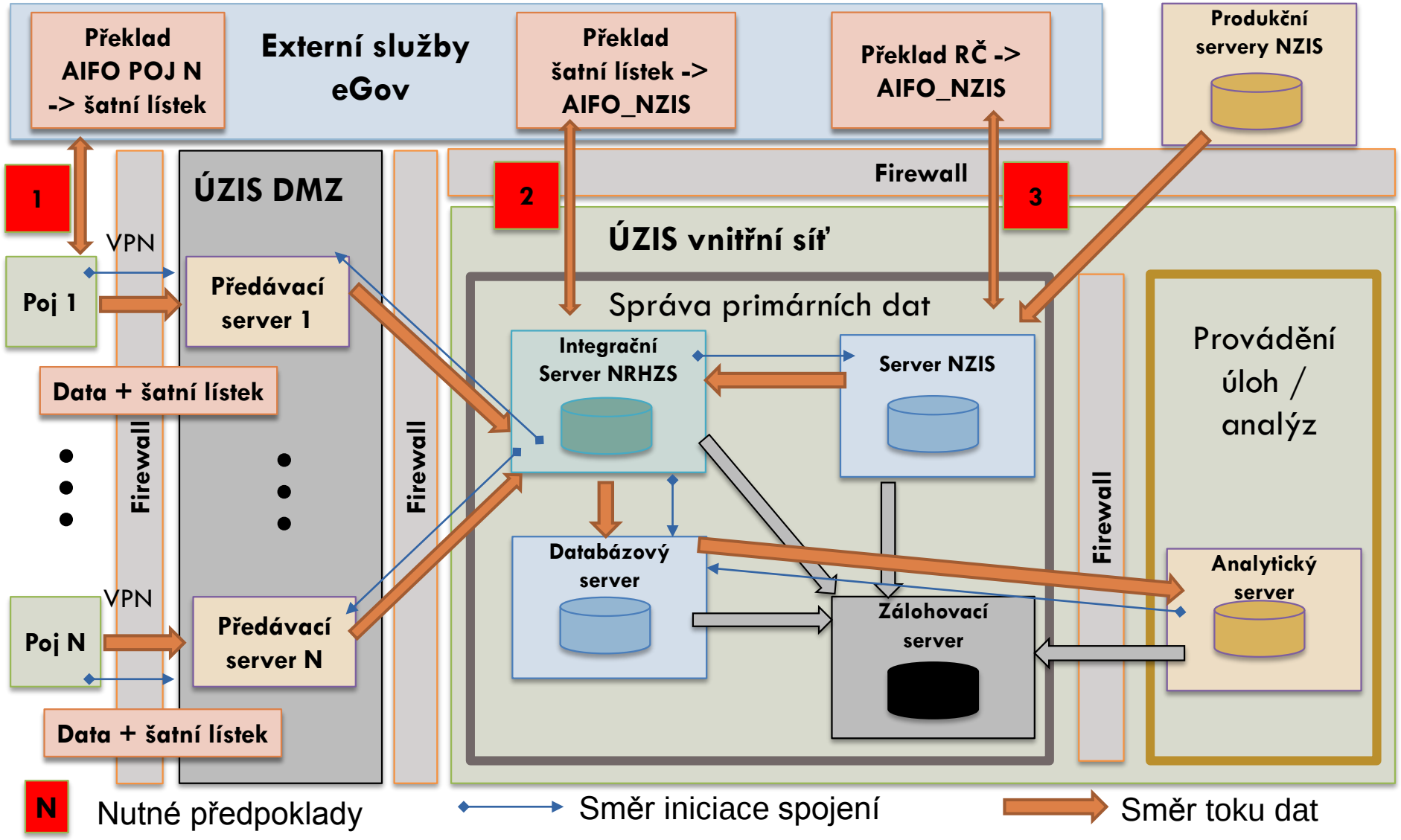
Například analogové nástroje zpracování, jako jsou kartotéky a jiné způsoby zpracování informací

Komunikační infrastruktura

Mobilní zařízení, ostatní technické nosiče infomrací

v01

Národní registr hrazených zdravotních služeb



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Diskuse a dotazy

Kontakt:

Mgr. JUDr. Vladimira Těšitelová
vladimira.tesitelova@uzis.cz
tel. 224 972 883, 224 972 712

ÚZIS ČR