Centrum pro rozvoj technologické platformy registrů Národního zdravotnického informačního systému,
modernizace vytěžování jejich obsahu a rozšíření jejich informační kapacity.
Rozvoj technologické platformy NZIS — CZ.03.4.74/0.0/0.0/15_019/0002748

Rozvoj technologické platformy NZIS

Nařízení EU na ochranu osobních údajů/Stávající příprava rezortu na GDPR

Mgr. JUDr. Vladimíra Těšitelová
Statutární zástupce ředitele ÚZIS ČR

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Ústav zdravotnických informací a statistiky České republiky
Institut biostatistiky a analýz Masarykovy univerzity
Společné pracoviště

Obsah a cíle

1. Základní informace
2. Jaké změny přináší
3. Některá nová konkrétní práva subjektu údajů a povinnosti správců/zpracovatelů
4. Příprava rezortu zdravotnictví
5. Praktické dopady - implementace, zkušenosti ÚZIS ČR

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Základní informace GDPR

- oficiální název - Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů),
- účinnost – od 25.5.2018
- jedná se o obecné nařízení – účinnost automaticky v plném rozsahu s výjimkou ustanovení, kdy je členským státům umožněno/uloženo upravit si je na vnitrostátní úrovni (cca 50)

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Vazba GDPR na vnitrostátní právo ČR

- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdější pozdějších předpisů, nyní v legislativním procesu novela zákona („adaptační zákon“)
- zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) ve znění pozdějších předpisů - explicitně pro rezort zdravotnictví, zejména ustanovení týkající se zdravotnické dokumentace či NZIS,
- zákon č. 373/2011 Sb., o specifických zdravotních službách a podmínkách jejich poskytování (zákon o specifických zdravotních službách)

Vazba GDPR na vnitrostátní právo ČR

- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdější pozdějších předpisů,
- zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) ve znění pozdějších předpisů - explicitně pro rezort zdravotnictví, zejména ustanovení týkající se zdravotnické dokumentace či NZIS,
- zákon č. 373/2011 Sb., o specifických zdravotních službách a podmínkách jejich poskytování (zákon o specifických zdravotních službách)

Vazba GDPR na vnitrostátní právo ČR

- zákon č. 374/2011 Sb., o zdravotnické záchranné službě
- zákon č. 89/1995 Sb., o státní statistické službě,
- zákon č. 262/2006 Sb., zákoník práce
- zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů
- zákon č. 378/2007 Sb., o léčivech
- zákon č. 123/2000 Sb., o zdravotnických prostředcích
- zákon č. 258/2000 Sb., o ochraně veřejného zdraví

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Vazba GDPR na vnitrostátní právo ČR

- zákon č. 40/2009 Sb., trestní zákoník
- zákon č. 285/2002 Sb., o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů (transplantační zákon)
- zákon č.296/2008 Sb., o zajištění jakosti a bezpečnosti lidských tkání a buněk určených k použití u člověka a o změně souvisejících zákonů (zákon o lidských tkáních a buňkách) atd.

Plus prováděcí předpisy k výše uvedeným zákonným normám.

Obsah a součásti GDPR

Recitály 1-173
obsahuje zásady a definice
jednotlivá ustanovení je nutno vykládat v souladu s recitály

Kapitoly I-XI
Upravují jednotlivé oblasti úpravy
Od obecných ustanovení - po závěrečná ustanovení

Články 1-99
jednotlivá pravidla a regulace
50 výjimek, resp.možností či povinností regulací pro vnitrostátní právo

Ucelená soustava závazných pravidel

Pracovní skupina WP 29
Publikuje výkladové materiály
Publikovány 3 výkladové materiály
4/2017 publikováno doporučení k DPIA

Co nového přináší GDPR

1. přesnější definice
2. transparentnost a souhlas subjektu údajů
3. posílená práva subjektu údajů
4. rozšířené povinnosti správců/zpracovatelů
5. rozšířené povinnosti /oprávnění Úřadu pro dozor
6. odpovědnost, řízení rizik, reporting
7. hlášení bezpečnostních incidentů
8. vyšší sankce

GDPR není revolucí je evolučním procesem příležitostí

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Co nového přináší GDPR/Na co se GDPR nevztahuje ?

1. na osobní údaje právnických osob
2. na anonymní údaje
3. na údaje o zemřelých
4. na otázky nespadající do působnosti EU – např. národní bezpečnost
5. fyzickou osobou v rámci činností osobní povahy nebo činnosti prováděné výhradně v domácnosti
6. prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.

GDPR není revolucí je evolučním procesem příležitostí

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

ÚZIS IBA

Kdy je zpracování dle GDPR zákonné ?

, pokud je činěno:

- se souhlasem subjektu údajů,
- na základě zákona,
- je nezbytné v souvislosti s plněním smlouvy nebo úmyslem smlouvu uzavřít,
- plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,
- je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (např. život, humanitární účely, epidemie, humanitární účely, katastrofy).

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Posílení práv subjektu údajů

- právo subjektu údajů na transparentní, srozumitelné a snadno přístupným způsobem dostupné informace o osobních údajích, které byly získány se souhlasem i bez souhlasu (čl. 12)
- právo subjektu údajů na poskytnutí informací v rozsahu odst. 1 písm a)- f) i o dalším účelům zpracování u osobních údajů, které byly získány SE SOUHLASEM (čl. 13)
- právo subjektu údajů na přístup k osobním údajům (čl. 15
- právo subjektu údajů na opravu, právo subjektu údajů na doplnění neúplných osobních údajů (čl. 16)

Posílení práv subjektu údajů

- právo na výmaz („právo být zapomenut“)(čl. 17 odst. 1)
- právo na omezení zpracování (čl. 18)
- oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování (čl. 19)
- právo na přenositelnost údajů (čl. 20)
- právo vznést námitku (čl. 21)
- právo na to, aby subjekt údajů nebyl předmětem automatizovaného rozhodování, vč. Profilování (čl. 22)
- právo na podání stížnosti u dozorového úřadu (čl. 77)
- právo na účinnou soudní ochranu vůči dozorovému úřadu, správci i zpracovateli (čl. 78 a 79)

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Posílení práv subjektu údajů

- právo na to být zastoupen neziskovým subjektem, organizací nebo sdružením (čl. 80)
- právo na náhradu újmy (čl. 82)

Výjimky/odchylky pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely (čl. 89).

Specifika pro zdravotnictví.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Posílení práv subjektu údajů/dopady pro správce/zpracovatele

Čl. 12
právo subjektu údajů na transparentní, srozumitelné a snadno přístupným způsobem dostupné informace o osobních údajích, které byly získány se souhlasem i bez souhlasu

Dopad
povinnost správce informovat subjekt údajů transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace dle čl. 13,14, 15-22 a 34. informace písemná, elektronická a na žádost ústní.

Poznámka nezapomenout !
Zavést mechanismus vyřizování žádostí.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Posílení práv subjektu údajů/dopady pro správce/zpracovatele

čl. 13
právo subjektu údajů na poskytnutí informací v rozsahu odst. 1 písm a)- f) i o dalším účelům zpracování u osobních údajů, které byly získány SE SOUHLASEM
správce musí tyto informace poskytnout v okamžiku získání osobních údajů s výjimkou případů, že je již subjekt údajů má
jedná se o novou povinnost, kterou je nutné zohlednit.
Dopad:
Nutno zavést systém zajištění informovanosti pacientů.

čl. 14
právo subjektu údajů na poskytnutí informací, pokud byly získány BEZ SOUHLASU ÚDAJŮ
Vzhledem k tomu, že jsou tyto údaje stanoveny zákonem je toto právo omezeno.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Posílení práv subjektu údajů/dopady pro správce/zpracovatele

čl. 15
právo subjektu údajů na přístup k osobním údajům
povinnost subjektu údajů na základě jeho žádosti sdělit, resp. údaje předat.

Poznámka nezapomenout !
Zavést mechanismus vyřizování žádostí.

čl. 16
právo subjektu údajů na opravu
právo subjektu údajů na doplnění neúplných osobních údajů
bez zbytečného odkladu opraví nepřesné osobní údaje, které se týkají subjektu údajů

čl. 17 odst. 1
právo na výmaz („právo být zapomenut“)
Vzhledem k tomu, že jsou tyto údaje stanoveny zákonem je toto právo omezeno.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

ÚZIS IBA

Posílení práv subjektu údajů/dopady pro správce/zpracovatele

čl. 18

právo na omezení zpracování

- Správce omezí zpracování, v kterémkoli z těchto případů:
- subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;
- zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
- subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

ÚZIS IBA

Posílení práv subjektu údajů/dopady pro správce/zpracovatele

čl. 19
oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

- subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;
- zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
- subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

ÚZIS IBA

Posílení práv subjektu údajů/dopady pro správce/zpracovatele

čl. 20
právo na přenositelnost údajů

Předávání osobních údajů jedním správcem správci druhému (za předpokladu technické proveditelnosti) lze realizovat pouze za kumulativního splnění 2 podmínek:

- zpracování založeno na souhlasu nebo smlouvě a
- jedná se o automatizované zpracování

WP 29 vydalo stanovisko, jako jediné nebylo doposud revidováno.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Posílení práv subjektu údajů/dopady pro správce/zpracovatele

čl. 21

právo vznést námitku

Správcem těchto údajů, které je nezbytné pro účely oprávněných zájmů Správce či třetí strany (viz níže), vč. profilování (profilováním se rozumí individuální automatizované rozhodování) založeného na tomto zpracování. Jedná se konkrétně např. o:

- ochranu majetku (kamerový systémy, prokázání totožnosti)
- přímý marketing (v takových mezích, které můžete očekávat) a
- předávání údajů ve skupině pro administrativní účely
- pohledávky, soudní spory stížnosti.

Námitku je možné vznést ústně či písemně u Správce.

Poznámka nezapomenout !

Zavést mechanismus poučení subjektu údajů o možnosti podat stížnost nebo vznést námitku.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

ÚZIS IBA

Posílení práv subjektu údajů/dopady pro správce/zpracovatele

čl. 22

právo na to, aby subjekt údajů nebyl předmětem automatizovaného rozhodování, vč. profilování

Správce nesmí provádět výhradně automatizované individuální rozhodování, vč. profilování, s následujícími výjimkami:

- je zákonem stanoveno,
- je založeno na souhlasu subjektu
- je nezbytné pro uzavření smlouvy nebo jejího plnění se subjektem.

Definice profilování čl. 4 odst. 4
jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu - **typický příklad web**.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Posílení práv subjektu údajů/dopady pro správce/zpracovatele

čl. 77
právo podat stížnost u dozorového úřadu

Správce se stává součástí, resp. předmětem šetření.

Poznámka nezapomenout !

Zavést mechanismus poučení subjektu údajů o možnosti podat stížnost nebo vznést námitku.

Máte právo podat stížnost u dozorového úřadu, a to v případě, že se domníváte, že zpracováním osobních údajů dochází k porušení GDPR. Stížnost můžete podat u dozorového úřadu:

a) v místě svého obvyklého bydliště,
b) místě výkonu zaměstnání nebo
c) místě, kde došlo k údajnému porušení.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Posílení práv subjektu údajů/dopady pro správce/zpracovatele

čl. 78
právo na účinnou soudní ochranu vůči správci nebo zpracovateli

Správce se stává stranou soudního sporu.

čl. 80
právo na to být zastoupen neziskovým subjektem, organizací nebo sdružením

Povinnost správce jednat s takovýmto subjektem, který zastupuje subjekt údajů.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Posílení práv subjektu údajů/dopady pro správce/zpracovatele

čl. 82.
právo na náhradu újmy

Sankce jsou „dvourychlostní“ „dvoustupňové“.

Za porušení některých ustanovení lze uložit správní pokuty až do výše 10 000 000 EUR, resp. 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 2 %, resp. 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Posílení práv subjektu údajů/dopady pro správce/zpracovatele

čl. 82.

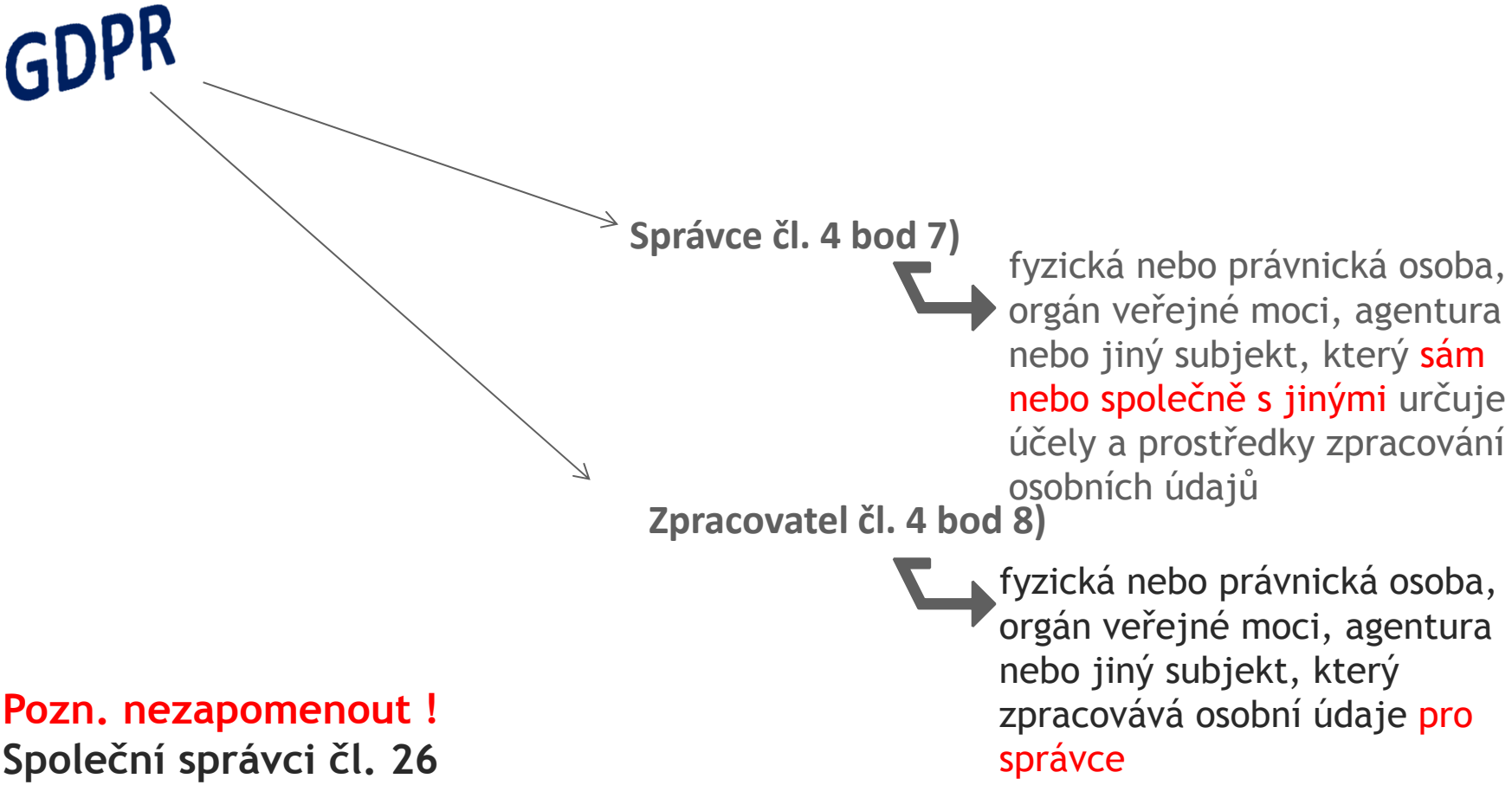
právo na náhradu újmy

Vyšší sankce jsou ukládány za porušení:

- základních zásad zpracování,
- práv subjektu údajů,
- předání osobních údajů do třetích zemí a mezinárodním organizacím,
- nesplnění příkazu dozorového úřadu dočasného omezení zpracování a
- porušení jakékoli povinnosti vyplývající z právních předpisů členského státu dle kapitoly IX (zpracování a svoboda projevu informací, přístup veřejnosti k úředním dokumentům, zpracování národních identifikačních čísel, zpracování v souvislosti se zaměstnáním, pro účely archivace ve veřejném zájmu, pro vědecký a historický výzkum a pro statistické účely).

Členské státy mohou stanovit i jiné sankce.

Definice správce a zpracovatele dle GDPR



Pozn. nezapomenout !

Společní správci čl. 26

„Ze zpracovatele správcem“ čl. 28 odst. 10 Pokud zpracovatel poruší toto nařízení tím, že určí účely a prostředky zpracování, považuje se ve vztahu k takovému zpracování **za správce.**

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Rozdělení povinností správce/zpracovatele

I. Obecné povinnosti

Jasně definované povinnosti správce/zpracovatele vyplývající z jednotlivých ustanovení GDPR, s výjimkou povinností vyplývajících z práv subjektu údajů

II. Povinnosti korespondující s rozšířenými právy a povinnostmi subjektu údajů

Okruh povinností, které vyplývají z rozšířeného okruhu práv subjektu údajů

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Obecné povinnosti správce/zpracovatele

- zpracovávat osobní údaje v souladu s GDPR (čl. 24)
- záměrná a standardní ochrana osobních údajů (čl. 25)
- smlouvy o zpracování čl. 28 a ostatní)
- zpracování z pověření správce nebo zpracovatele (čl. 29)
- záznamy o činnostech zpracování (čl. 30)
- spolupráce s dozorovým úřadem (čl. 31)
- zabezpečení zpracování (čl. 32)
- Ohlášení porušení zabezpečení osobních údajů dozorovému úřadu (čl. 33)

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Obecné povinnosti správce/zpracovatele

- Ohlášení případů porušení zabezpečení osobních údajů subjektu údajů (čl. 34)
- Posouzení vlivu na ochranu osobních údajů a předchozí konzultace (čl. 35)
- Jmenování pověřence na ochranu osobních údajů (čl. 37 a 39)
- Předávání osobních údajů do třetích zemí a mezinárodním organizacím (čl. 44)

Příprava rezortu

- analýza právní úpravy ČR ve vazbě na výjimky umožňující výjimky z jednotlivých ustanovení GDPR
- zpracování jednotné metodologie implementace GDPR pro PŘO („Brožura“)
- zavedení šablon
- Etc……..

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Postup implementace GDPR v přímo řízených organizacích MZ

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

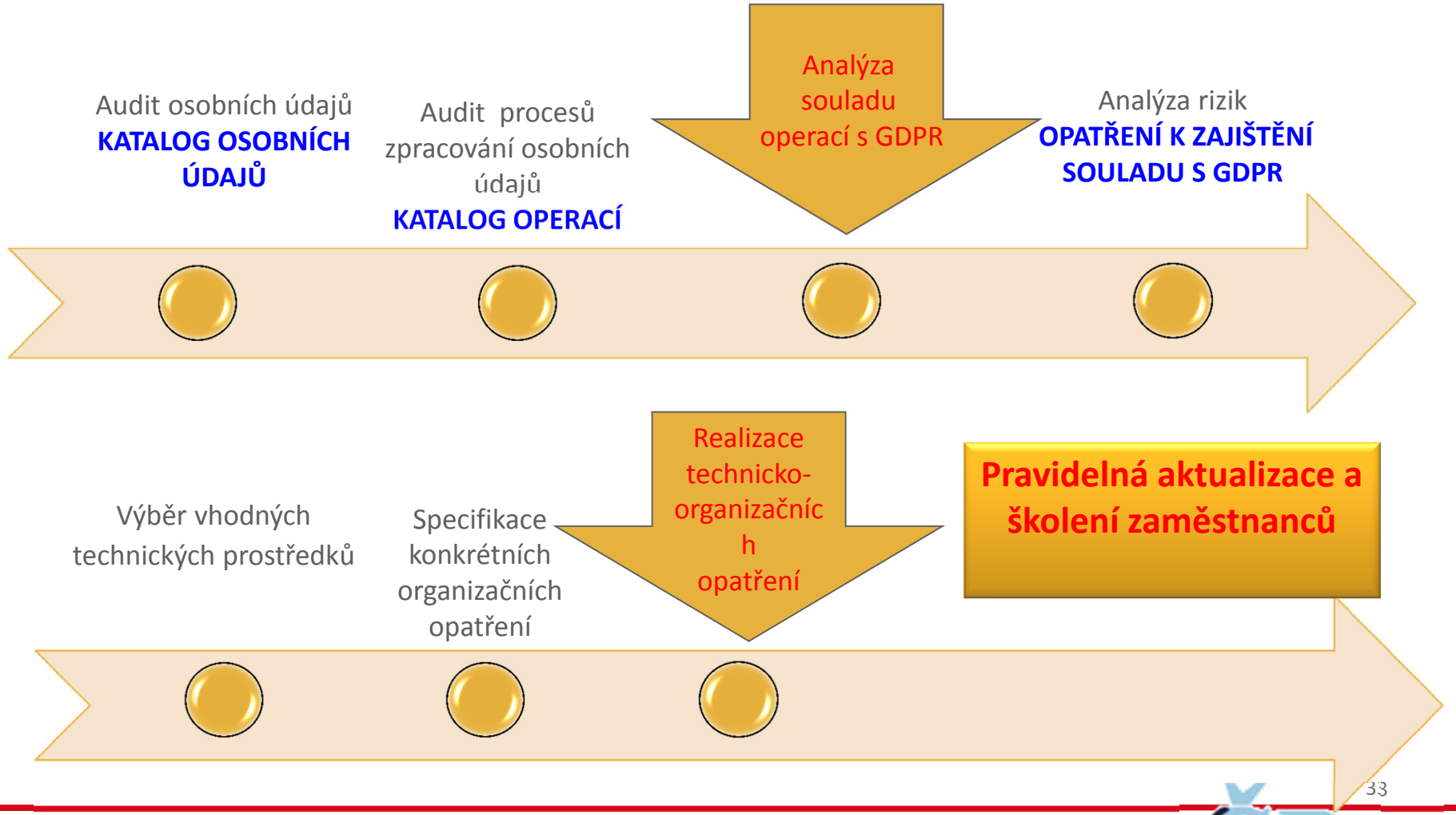
JUDr. Radek Policar

Mgr. JUDr. Vladimíra Těšitelová

23.8.2017

Seminář k GDPR pro PŘO Ministerstva zdravotnictví

Základní kroky implementace GDPR



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

ÚZIS

Další postup MZ ČR

- Dopracování brožury Potup implementace v PŘO;
- Kurz pro pověřence pro ochranu osobních údajů,
- Zpracování katalogu osobních údajů a operací ze strany PŘO;
- Etc……..

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Implementace GDPR v podmínkách ÚZIS ČR

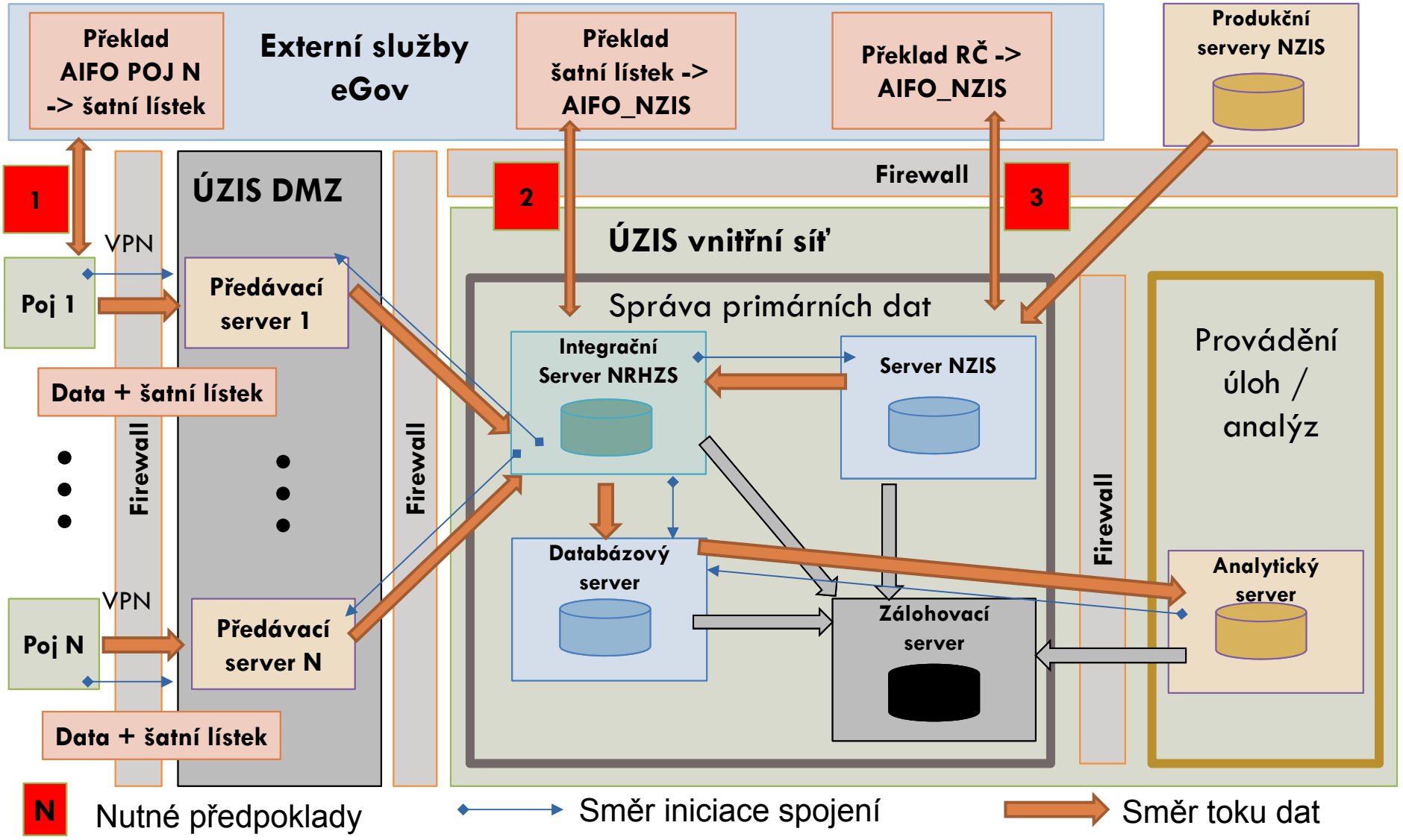
- jmenován pověřenec pro ochranu osobních údajů;
- již v průběhu legislativního procesu novely zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) realizovaný zákonem č. 147/2016 Sb., i jeho prováděcí vyhlášky č. 373/2016 Sb., o předávaní údajů 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.

…. A pokračujeme dále

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Rozvoj technologické platformy NZIS

Národní registr hrazených zdravotních služeb



Diskuze

Kontakt:

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