FAKULTNÍ NEMOCNICE BRNO

Dopady GDPR na elektronizaci zdravotnictví

TELEMEDICÍNA BRNO 2019

Alena Tobiášová

Vymezení tématu

- Smlouva o zpracování
- Zabezpečení zpracování
- Posouzení vlivu na ochranu osobních údajů
- Kodex chování

Smlouva o zpracování

SPRÁVCE x ZPRACOVATEL

- správce
  - určuje účely a prostředky zpracování osobních údajů
  - jsou-li účely a prostředky zpracování určeny právem, může být správce určený právem
- zpracovatel
  - zpracovává osobní údaje pro správce dle jeho pokynů

Smlouva o zpracování

- Zpracování zpracovatelem se řídí smlouvou
  - předmět
  - doba trvání zpracování
  - povaha a účel zpracování
  - typ osobních údajů
  - kategorie subjektů údajů
  - povinnosti a práva správce
- Smlouva v písemné formě

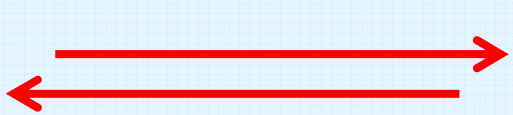
Závazek zpracovatele vůči správci

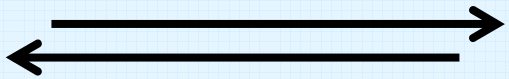
- zpracovávání pouze na základě doložených pokynů správce
- osoby oprávněné zpracovávat jsou zavázány mlčenlivostí (závazek, zákon)
- vhodná TOO k zajištění zabezpečení
- zapojení do zpracování dalšího zpracovatele s předchozím povolení správce (smlouva)
- součinnost - žádosti o výkon práv subjektu
- naložení s OÚ po ukončení poskytování služeb
- informace potřebné k doložení plnění povinností (audity, inspekce)

Zpracování z pověření

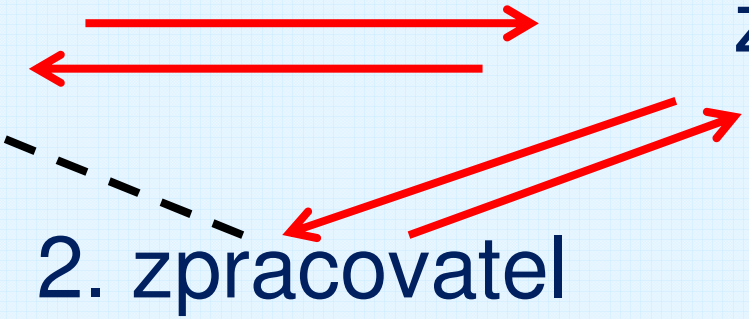
- zpracovatel a jakákoliv osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, může tyto osobní údaje zpracovávat pouze na pokyn správce, ledaže jí jejich zpracování ukládá právo

Zpracovatelská smlouva

správce  zpracovatel

správce  správce

správce pověření

správce  zpracovatel

2. zpracovatel

Zabezpečení zpracování

Zabezpečení zpracování

- Povinnost správce / zpracovatele:
  - posoudit rizika pro práva svobody fyzických osob
  - přijmout adekvátní bezpečnostní opatření
- Rizika
  - ➢ vznik majetkové, nemajetkové újmy
    - diskriminace, krádeže, zneužití identity, finanční ztráty, poškození pověsti, ztráty důvěrnosti citlivých údajů…

Datový a procesní audit

- **Technická analýza rizik**
  - Identifikace a ohodnocení rizik
  - Stanovení TOO ke zvládání rizik
- **Právní analýza rizik**
  - Identifikace práv a svobod
  - Identifikace a ohodnocení rizik
    - narušení důvěrnosti
    - narušení integrity
    - narušení dostupnosti
  - Stanovení TOO ke zvládání rizik

Označení aktiva - název procesu	Subjekt údajů	Účel zpracování	Forma zpracování	Zpracováváno se souhlasem subjektu údajů Ano / Ne	Údaje jsou zpracovávány pro…				Typ a rozsah údajů				Zásady GDPR
					Vlastní potřebu		Externí subjekt		Jméno a příjmení	……	Biometrické údaje	Další - konkretizace	
					Ano / Ne	Anonymizované Ano / Ne	Název externího subjektu	Anonymizované Ano / Ne					
zdravotnická dokumentace	pacient, osoby v anamnéze, zdravotničtí pracovníci	poskytování zdrav. služeb	E, L	Ano, Ne	Ano	Ne	oprávněné subjekty	Ano, Ne	Ano	……	Ano	bydliště, státní příslušnost, ID pacienta, číslo pojištěnce	Ano
evidence smluv	smluvní strany – FO a její zaměstnanci, vlastní zaměstnanci	naplnění smluvních vztahů	E, L	Ne	Ano	Ne			Ano	……		bydliště smluvní strany, telefon a e-mail zaměstnance, e-mail smluvní strany	Ano
osobní spisy zaměstnanců	zaměstnanci, další zúčastněné osoby	evidence zaměstnanců - výkon personální agendy	E, L	Ano, Ne	Ano	Ne			Ano	……		bydliště, osobní číslo, telefon, e-mail, rodinný stav, státní příslušnost, osobní údaje dětí a dalších osob	NE (!)

Matice zranitelností a katalog hrozeb			Práva a svobody										
Aktiva	**Hrozby**		**Právo na soukromí**	**Právo na ochranu cti a důstojnosti**	**Právo na informační sebeurčení**	**Právo na život**	**Právo na duševní a tělesnou integritu**	**Právo na informace**	**Právo na ochranu OÚ**	**Zákaz diskriminace**	**Ochrana identity**	**Hmotné ztráty**	**Neoprávněné zrušení pseudon.**
Popis	**Hrozba**	**Hodnota**	**3**	**3**	**1**	**5**	**4**	**2**	**3**	**2**	**5**	**3**	**3**
zdravotnická dokumentace	Narušení důvěrnosti včetně neoprávněného zpřístupnění osobních údajů a neoprávněného přístupu k osobním údajům	2	5	4	2	1	1	0	5	0	0	2	1
	Narušení integrity včetně pozměnění osobních údajů	1	0	3	0	3	5	1	2	0	0	0	0
	Narušení dostupnosti včetně náhodného nebo protiprávního zničení osobních údajů	1	0	0	0	3	3	3	0	0	0	0	0
	Ztráta osobních údajů	1	5	4	2	3	3	3	5	0	0	2	1
evidence smluv	Narušení důvěrnosti	2	3	2	1	0	0	0	3	0	0	1	1
	Narušení integrity	1	0	0	0	0	0	0	0	0	0	5	1
	Narušení dostupnosti	2	0	0	0	0	0	1	0	0	0	1	0
	Ztráta osobních údajů	1	3	2	1	0	0	1	3	0	0	1	1
osobní spisy zaměstnanců	Narušení důvěrnosti	2	5	2	4	0	0	0	5	2	2	0	4
	Narušení integrity	1	0	0	0	0	0	0	0	2	2	2	0
	Narušení dostupnosti	1	0	0	0	0	0	0	0	0	0	2	0
	Ztráta osobních údajů	1	5	2	4	0	0	0	5	2	2	2	4

Technická a organizační opatření

- Smyslem TOO je zabezpečení ochrany osobních údajů a soulad zpracování s GDPR
- Cílem je snížit rizika na přijatelnou úroveň
- Opatření přiměřená stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování
- Průběžný proces

Technická opatření

např.:

- ✓ šifrování, pseudonymizace
- ✓ zabezpečení sítě, HW, SW tech. prostředky
- ✓ autentizace a autorizace pro přístup
- ✓ identifikace a monitorování vstupu do určených prostor – elektronické karty, kamerový systém, …
- ✓ materiální zajištění – uzamykaní, trezor, mříže, …
- ✓ SW pro pravidelný monitoring administrativních úkonů a přístupů k prostředkům

Organizační opatření

např.:

- ✓ systematické zvyšování právního vědomí
- ✓ popis procesů, stanovení kompetencí, odpovědnosti, sankcí, audity (řídící dokumenty)
- ✓ zavázání mlčenlivostí
- ✓ definování přístupových práv do IS – rozsah, správa hesla, logování
- ✓ pravidla nakládání se zdravotnickou dokumentací
- ✓ skartace os. údajů – povinnost (vč. elektronické)

Ohlašování případů porušení zabezpečení osobních údajů

➢ Povinnost správce

- Dozorovému úřadu
  - ➢ bez zbytečného odkladu, do 72 hodin od okamžiku, kdy se o porušení dozvěděl /důvody zpoždění
    - výjimka - není riziko pro práva a svobody fyzických osob
    - povinnost správce dokumentovat veškeré případy porušení zabezpečení osobních údajů
- Subjektu údajů
  - ➢ pravděpodobnost vysokého rizika pro práva a svobody fyzických osob
    - výjimka – TOO stávající / přijatá znemožňují zneužití

Posouzení vlivu na ochranu osobních údajů

*(**D**ata **P**rotection **I**mpact **A**ssessment)*

Posouzení vlivu na ochranu osobních údajů (DPIA)

- Pokud je pravděpodobné, že určitý druh zpracování, zejm. při využití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody
  - ✓ rozsáhlé zpracování zvláštních kategorií údajů
  - ✓ rozsáhlé systematické monitorování veřejně přístupných prostorů
  - ✓ …

Vysoké riziko pro práva a svobody

Kritéria (Evropský sbor pro ochranu os. údajů)

- systematické monitorování
- zpracování citlivých údajů
- zpracování údajů v rozsáhlém měřítku
- přiřazování či slučování datových souborů
- …

Obsah posouzení

- ✓ systematický popis operací
- ✓ posouzení nezbytnosti a přiměřenosti operací
- ✓ posouzení rizik pro práva a svobody
- ✓ plánovaná opatření k řešení rizik

- posudek pověřence pro ochranu osobních údajů
- konzultace před zpracováním s dozorovým úřadem

Kodex chování

Účel kodexu chování

- prokázání souladu operací zpracování osobních údajů s GDPR
- dobrovolný systém samoregulace
- řešení nejasností a specifik, které vznikají při zpracování osobních údajů v rámci daného odvětví (např. zdravotnictví)
- upřesňování povinnosti správců a zpracovatelů s přihlédnutím k riziku, které ze zpracování pravděpodobně vyplyne pro práva a svobody fyzických osob

„*Správce*“ kodexu chování

- Sdružení / jiné subjekty zastupující různé kategorie správců / zpracovatelů
  - mohou vypracovávat kodex chování s cílem upřesnit uplatňování nařízení
  - zaváží se k jeho aktualizace (vývoj legislativy, změny postupů správců, vývoji IT …)
  - závazek správce nebo zpracovatele k dodržování kodexu chování je dobrovolný

Postup

- návrh kodexu či návrhy na úpravu či rozšíření kodexu se předkládá dozorovému úřadu
- dozorový úřad posoudí, zda je daný návrh kodexu nebo návrh na úpravu či rozšíření kodexu v souladu s nařízením
  - ➢ schválí, zaregistruje a zveřejní
- týká-li se činností zpracování v několika členských státech - Evropský sbor pro ochranu osobních údajů
- po schválení dozorovým úřadem se mohou přihlásit ke kodexu jednotliví správci / zpracovatelé

Monitorování schválených kodexů chování

- může provádět subjekt
  - ✓ má příslušnou úroveň odborných znalostí
  - ✓ je pro tento účel akreditován dozorovým úřadem
- akreditace subjektu
  - ✓ prokázal nezávislost a odborné znalosti
  - ✓ stanovil postupy umožňující posoudit způsobilost dotčených správců a zpracovatelů
  - ✓ stanovil postupy a struktury pro řešení stížností
  - ✓ prokázal, že jeho úkoly a povinnosti nevedou ke střetu zájmů

Kodex(y) chování a zdravotnictví

Příležitost k řešení specifik poskytovatelů ZS

- Ministerstvo zdravotnictví
- ANČR, AČMN, SPL ČR …
- … ?

✓ Jednotná aplikace jasných pravidel v rezortu zdravotnictví ⟹ v EU

Děkuji za pozornost

JUDr. Alena Tobiášová, MBA

tobiasova.alena@fnbrno.cz