

(Snad) praktický pohled na GDPR

Tomáš Nielsen

NIELSEN MEINL, advokátní kancelář, s.r.o.

GDPR

- Nařízení EP a Rady č. 2016/679 z 27. 4. 2016
- Účinnost od 25. 5. 2018
- Stanoví závazná pravidla pro zpracování osobních údajů
 - Správci či zpracovatelé s provozovnou na území EU
 - Subjektů údajů nacházejících se na území EU (nabídka zboží nebo služeb nebo monitorování chování)
 - Mimo EU, pokud se uplatní právo EU dle mezinárodní smlouvy

GDPR – co je nového?

- Bližší vymezení již existujících povinností
- Nové povinnosti správců a zpracovatelů
- Nová práva subjektů údajů
- Nové instituty (DPIA, DPO...)
- Větší tlak na interní procesy (snaha nahradit formální přístup přístupem materiálním)
- Zaniká povinnost předchozí registrace u ÚOOÚ

Standardní výchozí stav

- Často první kontakt s ochranou OÚ
- Neznalost nových povinností
- Neznalost vlastního prostředí
- Chybný pohled na výklad „zpracovatele“
- Povědomí o GDPR aneb mýty a legendy 2018

Základní pojmy

- Osobní údaj

*„**Veškeré informace** o identifikované **nebo identifikovatelné** fyzické osobě; identifikovatelnou je osoba, kterou lze přímo či **nepřímo** identifikovat, **zejména** odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“*

Základní pojmy

- Specifické osobní údaje:
 - Zvláštní kategorie osobních údajů:
 - údaje o rasovém či etnickém původu, politických názorech, náboženství či filozofii, členství v odborech
 - genetické a biometrické údaje sloužící k identifikaci
 - údaje o zdravotním stavu či sexuálním životě / orientaci
- Údaje o rozsudcích v trestních věcech a trestných činech

Základní pojmy

- Zpracování

*„**Jakákoliv** operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, **jako je** shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo **jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení**“*

Základní pojmy

- Správce

*„Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými **určuje účely** a **prostředky** zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení “*

Základní pojmy

- Zpracovatel

*„Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který **zpracovává** osobní údaje pro správce“*

Neznalost nových povinností

- Informační povinnost i pro zpracování bez souhlasu
- Vedení záznamů o zpracování
- Proces na realizaci práv subjektů údajů
- Hlášení incidentů
- Odpovědnost za aktuálnost údajů
- Existence podrobné smlouvy o zpracování
- Analýza rizik zpracování / DPIA
- DPO

Povinnosti správce

- Stanovit právní základ, účel a dobu zpracování
- Zajistit technická a organizační opatření na ochranu osobních údajů (pseudonymizace, testování, důvěrnost a dostupnost)
- Určit:
 - Zda budou informace předávány jiným osobám
 - Zda budou informace předávány mimo EU
 - Jak bude subjektů údajů realizovat svá práva
 - Jak bude zpracování evidováno
 - Zda bude docházet k automatizovanému rozhodování, vč. profilování

Povinnosti správce

- Informovat řádně subjekty údajů
- Zpracovávat údaje pouze v souladu s účelem a po určenou dobu a pouze tak, jak informoval subjekt údajů
- Zajistit realizaci práv subjektů údajů
- V případě užití zpracovatele uzavřít písemnou smlouvu o zpracování (včetně elektronické formy)
- Spolupráce s dozorovým úřadem
- Oznamovat případy porušení zabezpečení osobních údajů
- V případě zvýšeného rizika pro práva subjektu údajů – DPIA
- V případě splnění podmínek GDPR – jmenovat DPO

Práva subjektů údajů

- Právo na přístup k údajům
- Právo na informace
- Právo na vysvětlení
- Právo na odstranění závadného stavu
- Právo na opravu údajů
- Právo na omezení zpracování
- **Právo na výmaz**
- **Právo na přenositelnost údajů**
- **Právo vznést námitku**
- **Právo na lidský zásah** (v případě automatizovaného rozhodování)

Neznalost prostředí - stav

- Jen rámcový přehled o zpracovávaných OÚ a o formách zpracování
- Absence kategorizace OÚ, důvodů a účelů zpracování, stanovení doby archivace
- Neurčité povědomí o příjemcích údajů (zpracovatelé)

Neznalost prostředí - řešení

- Správné (funkční) zmapování operací s OÚ
- Definice kategorií OÚ, důvodů a účelů zpracování, stanovení doby archivace
- Identifikace třetích osob, které přicházejí do styku s OÚ, a ověření (příp. nastavení) správných vztahů

Chybný pohled na výklad „zpracovatele“ – stav

- Nemožnost přístupu k datům nemusí znamenat, že nejsem zpracovatelem (viz cloudové služby)
- Nejasné vymezení role při zpracování (správce / zpracovatel)
- Výsledkem může být zpracování OÚ v roli zpracovatele bez právního důvodu (smlouvy)

Chybný pohled na výklad „zpracovatele“ – řešení

- V rámci mapování operací určit, zda v našich systémech existují OÚ získané od třetích osob (příp. pro třetí osoby)
- Pokud ano, identifikovat, co se s OÚ děje
- Zjistit, kdo určuje účely a prostředky zpracování
- Pokud 3. osoba, jsme zpracovatelem (povinnost mít smlouvu o zpracování, ale odpovědnost jde primárně za správcem)

Povědomí o GDPR aneb mýty a legendy 2018 - stav

- Víra v mýtické informace
 - reálně nám hrozí pokuty 10-20 mio Eur
 - je povinnost vše šifrovat
 - je nutné implementovat IS, které přesně logují veškeré operace s OÚ
 - aktuálně zpracovávané OÚ musíme po 25. 5. smazat
 - od 25. 5. musíme mít nové souhlasy
 - profilování zákazníků je zakázáno
- Podceňování skutečnosti
 - stačí včas rozeslat oznámení subjektům OÚ
 - fakticky se nic nemění

Povědomí o GDPR aneb mýty a legendy 2018 - řešení

- Zorientovat se v operacích, při nichž dochází ke zpracování OÚ
- Získat informace o nových povinnostech z relevantních zdrojů
- Aplikovat standardní pravidla tam, kde je to možné
- Individuálně řešit složitější případy

Co dělat?

Základní principy

- Zákonnost, korektnost, transparentnost
- Legitimní účel
- **Přiměřenost a minimalizace** (rozsahu i doby)
- Správnost a aktuálnost
- Integrita a důvěrnost
- Odpovědnost a schopnost ji doložit

Právní základy zpracování

SOUHLAS	PLNĚNÍ ČI UZAVÍRÁNÍ SMLOUVY
PLNĚNÍ PRÁVNÍ POVINNOSTI	OCHRANA ŽIVOTNĚ DŮLEŽITÝCH ZÁJMŮ FO
VEŘEJNÝ ZÁJEM NEBO VÝKON VEŘEJNÉ MOCI	OPRÁVNĚNÝ ZÁJEM (SPRÁVCE ČI TŘETÍ OSOBY)

Účel a doba zpracování

- GDPR nestanoví účel ani dobu zpracování
- Obojí stanoví správce v souladu s:
 - Právním základem zpracování
 - Svými potřebami
 - Principy GDPR
 - Právními předpisy (např. v oblasti HR apod.)
 - **Zásadou přiměřenosti** (vztah osobní údaj v. jiný zájem/potřeba správce)

Informační povinnost

- Informovat řádně subjekty údajů
- Informace musí být:
 - Stručné
 - Transparentní
 - Srozumitelné
 - Snadno přístupné
 - Používat jasné a jednoduché jazykové prostředky

Kdy informovat?

- Údaje přímo od subjektu: v okamžiku získání
- Údaje od třetí osoby:
 - V přiměřené lhůtě od získání, nejpozději do 1 měsíce, ALE
 - Nejpozději při první komunikaci se subjektem údajů
 - Nejpozději při prvním zpřístupnění osobních údajů jinému příjemci

Záznamy o zpracování

- Kontaktní údaje správce, zástupce a pověřence
- Účely zpracování
- Kategorie subjektů údajů a kategorie údajů
- Kategorie příjemců osobních údajů (minulých i budoucích)
- Údaje o předání do třetích zemí
- Pokud je to možné, předvídanou dobu uložení osobních údajů
- Pokud je to možné, popis technických a organizačních bezpečnostních opatření

DPO

- Pověřenec pro ochranu osobních údajů – Data Protection Officer
- Povinný pro:
 - Orgány veřejné moci (s výjimkou soudů v rámci jejich pravomocí)
 - Hlavní činnost správce nebo zpracovatele vyžaduje pravidelné monitorování subjektů údajů, rozsáhlé zpracovávání citlivých osobních údajů apod.
- Musí být garantována nezávislost:
 - Přímo podřízen vrcholovému vedení
 - Nelze mu udílet pokyny týkající se výkonu svých pravomocí

DPO

- Hlavní úkoly:
 - Interní poradenství ohledně zpracování osobních údajů, vč. DPIA
 - Monitoring souladu s GDPR
 - Kontaktní místo pro subjekty údajů a dozorové úřady
 - Spolupráce s dozorovým úřadem
- Může jít o zaměstnance i externího poskytovatele služeb, fyzickou i právnickou osobu

DPO

- Kvalifikace
 - Konkrétní požadavky nejsou stanoveny
 - Musí mít odborné znalosti v oblasti vnitrostátní a evropské praxe a právních předpisů na ochranu údajů
 - Musí důkladně chápat nařízení o ochraně osobních údajů
 - Musí mít znalost podnikatelského odvětví a organizace
 - Porozumění informačním technologiím a zabezpečení osobních údajů
 - Porozumění prováděným operacím zpracování

DPO

- Některé povinnosti / odpovědnosti vyplynou i z novely zákona o ochraně osobních údajů (mlčenlivost pracovníků)
- Vodítka WP 29 (zajímavé jako „technické normy“)
- MV ČR stanoví zvláštní požadavky pro pověřence orgánů a organizací veřejné moci (ústřední orgány státní správy, samospráva apod.)

DPO

- **Přímo podřízen vrcholovým řídícím pracovníkům** správce nebo zprostředkovatele a má od nich dostávat aktivní podporu
- Měl by dostat odpovídající **podporu** z hlediska **finančních zdrojů, prostorů, vybavení** a případně **pracovníků**
- Všem zaměstnancům by mělo být **oficiálně oznámeno jmenování** pověřence
- Pověřenec **nesmí dostávat pokyny** od správců nebo zpracovatelů týkající se výkonu jeho funkce
- **Nemůže být propuštěn nebo sankcionován** v souvislosti s **řádným** výkonem úkolů pověřence pro ochranu osobních údajů
- Nemůže v rámci organizace zastávat pozici, ve které by **určoval účely a prostředky** zpracování osobních údajů (vedoucí pozice apod.)

Hlášení incidentů

- Nově – oznamovací povinnost porušení zabezpečení osobních údajů (dozorovému úřadu, v některých případech i subjektům údajů)
- Správce musí popsat incident, odhad důsledků porušení zabezpečení a přijatá opatření
- Lhůta: bez zbytečného odkladu, **nejpozději do 72 hodin**
- Povinnost evidovat případy porušení, účinky i přijatá opatření
- Povinnost není dána pokud je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob – **vždy potřeba vyhodnotit rizikovost incidentu**

Jak postupovat?

- Mapa procesů / transakcí
- Určení role při zpracování
- Vymezení kategorií osobních údajů
- Vymezení způsobu zpracování
- Identifikace právního základu pro zpracování, účelu a doby
- Identifikace všech příjemců (zpracovatelé, další správci apod.)
- Seznam seznamů, další vnitřní předpisy a dokumentace
- Nastavení funkčních vnitřních procesů (práva subjektů údajů apod.) a jejich kontrola
- Odpovědná osoba (kvaziDPO)
- Smlouvy, souhlasy, další dokumentace směrem ven

Několik bodů z praxe

Zajímavé výjimky

- Manuální zpracování osobních údajů určených pro evidenci (file system) – čl. 2
- Omezení povinností v případě, kdy není potřebná identifikace subjektů údajů – čl. 11
- Archivace ve veřejném zájmu, vědecký či historický výzkum, statistika
- Obhajoba právních nároků

Spolky

- Údaje členů orgánů – zákon je výslovně nevyžaduje, ale bez nich nelze plnit zákonné povinnosti – jde o splnění právní povinnosti
- Seznam členů – zákon jej nevyžaduje, ale může vyplývat ze stanov (§ 236 OZ) – odst. 2 ukládá povinnost přístupu k údajům člena ze seznamu členů – v takovém případě jde o splnění právní povinnosti
- Údaje statutárního (či jiného) zástupce člena – splnění právní povinnosti (zejm. zastupování člena na konferenci apod.)
- Seznam kontaktních osob členů – zákon jej nevyžaduje – oprávněný zájem
- Seznam dalších fyzických osob (technický zástupce, manažer jakosti) – zákon jej nevyžaduje – oprávněný zájem nebo souhlas (nutno zvážit)
- Možnost vydat kodex chování (čl. 40)

Subjekty posuzování shody

- Musí zpracovávat osobní údaje, aby byly schopny splnit některé právní povinnosti (§ 23 odst. 1 písm. b, e apod. zákona o posuzování shody) – prokázání absence konfliktu zájmů členů vedení a osob provádějících úkoly při posuzování shody; vybavenost pracovníky s odbornými znalostmi apod. – splnění právní povinnosti
- Musí zpracovávat osobní údaje z praktických důvodů (statutární zástupci dodavatelů/výrobců, kontaktní údaje, techničtí zástupci apod.) – oprávněný zájem
- Další (zaměstnanci, jiní zástupci zákazníků apod.) – nutno posoudit vždy individuálně

Předávání údajů do zahraničí

- Zůstávají stejná omezení
- Předávat údaje mimo EU lze pouze na základě existujících titulů:
 - Rozhodnutí Komise o odpovídající ochraně
 - Závazná podniková pravidla
 - Standardní doložky Komise či dozorového úřadu
 - Kodexy a osvědčení

Několik bodů k sankcím

- Neměly by být ukládány v nepřiměřené výši ALE
- Tendence sjednocovat výši sankcí v rámci EU
- Mají být odrazující
- Sankce nesmí být likvidační!
- Doporučuji soustředit se i na polehčující okolnosti – existuje řada lehčích nápravných opatření – napomenutí, uložení povinnosti, zákaz či omezení zpracování...

Další doporučení

- Sledujte stránky www.uoou.cz a EDPB (WP29)
- Sledujte články (epravo.cz, google apod.)
- Konzultujte nejasné věci s ÚOOÚ
- V případě nouze kontaktujte právníka



www.nielsenmeinl.cz

Kontakt

Tomáš Nielsen

+420 602 463 507

tnielsen@nielsenmeinl.com

NIELSEN MEINL, advokátní kancelář, s.r.o.

Žatecká 55/14, Praha 1