GDPR v české praxi – adaptační zákon a ochrana osobních údajů

Marie Šebelová, advokátka
Praha, 12. prosince 2018

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 115 579, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

Obsah

- Adaptační zákon
- Činnost ÚOOÚ
- GDPR – úvod, základní orientace
- Hlavní změny, které GDPR přináší
- Pojmy – osobní údaj, zpracování osobních údajů, subjekty zpracování, správce, zpracovatel
- Právní tituly zpracování OÚ podle GDPR
- Jednotlivé právní instituty dle GDPR – novinky, návody, vzory

Přijímací proces Zákona

Vláda předložila návrh Zákona sněmovně 28.3.2018 – tisk 138

- 1. čtení zákona ve sněmovně - 18.4.2018 na 12. schůzi
  - nebyl vysloven souhlas již v prvém čtení
  - návrh zákona byl přikázán k projednání výborům
- 2. čtení proběhlo 28.6.2018 na 16. schůzi
  - 18.9. zákon prošel obecnou a podrobnou rozpravou
  - podané pozměňovací návrhy
- 3. čtení proběhlo 5.12.2018
- Senát – do 30 dnů od předložení schválí nebo zamítne
- Prezident republiky – do 15 dnů podepíše nebo vrátí
- Účinnost Zákona – snad 1. polovina roku 2019

Adaptační zákon

Hlavním cílem adaptačního zákona je:

1) Adaptace Obecného nařízení 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Obecné nařízení)
2) Transpozice směrnice 2016/680, která upravuje zpracování osobních údajů justičními a policejními orgány

Adaptační zákon

Členění Zákona:

Hlava I – obecná ustanovení

Hlava II – adaptace Obecného nařízení

Díl 1 – ustanovení doplňující Obecné nařízené

Díl 2 – zpracování osobních údajů novináři

Hlava III – transpozice směrnice 2016/680 – upravuje zpracování osobních údajů justičními a policejními orgány

Hlava IV – zpracování osobních údajů, které je vyňato z působnosti práva EU a které se týká bezpečnosti a obrany ČR

Hlava V – postavení a kompetence nezávislého kontrolního úřadu – viz další příspěvek

Hlava VI – přestupky a pokuty

Jak Zákon doplňuje Obecné nařízení

Zákon upravuje zejména:

- Výjimku z povinnosti posuzování slučitelnosti účelů
- Způsobilost dítěte udělit souhlas se zpracováním OÚ
- Informační povinnost prostřednictvím dálkového přístupu
- Oznámení změny v evidenci
- Výjimku z povinnosti posouzení vlivu zpracování OÚ na ochranu OÚ
- Jmenování pověřence u orgánů veřejné moci a orgánů zřízených zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu
- Akreditace subjektů pro vydání osvědčení
- Zpracování OÚ prováděné pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu
- Činnost úřadu
- Zpracování OÚ justičními a policejními orgány

Adaptační zákon

Výjimka z povinnosti posuzování slučitelnosti účelů pro zvláště významná zpracování ve veřejném zájmu - recitál 50 GDPR

Rozšiřuje se slučitelnost účelů i na další případy kromě slučitelnosti zpracování pro vědecké nebo historické výzkumné účely, statistické účely a účely archivace ve veřejném zájmu

nově:

- obranné nebo bezpečností zájmy ČR
- veřejný pořádek a vnitřní bezpečnost
- ochrana nezávislosti soudů
- ochrana práv a svobod osob
- vymáhání soukromoprávních nároků

Adaptační zákon

Způsobilost dítěte udělit on-line souhlas se zpracováním OÚ

Snížení věkové hranice na 15 let

X

GDPR - 16 let

Je-li dítě daného věku způsobilé dát souhlas, je způsobilé i k jeho odvolání, uplatnění dalších práv (právo na výmaz)….

Adaptační zákon

Informační povinnost prostřednictvím dálkového přístupu

Toto ustanovení umožňuje splnit informační povinnost subjektů údajů (čl. 13, 14 GDPR) popisem a zveřejněním prostřednictvím dálkového přístupu – na Internetu.

Veřejná dostupnost stručné, srozumitelné a transparentní informace o zpracování je dostatečnou zárukou náležité informovanosti subjektů údajů. Ideální je odkázat na tuto veřejně dostupnou informaci při kontaktu se subjektem údajů.

Adaptační zákon

Výjimku z povinnosti posouzení vlivu zpracování OÚ na ochranu OÚ

Pokud právní předpis ukládá nějakou povinnost, jejíž součástí je i zpracování OÚ, nemusí správce provádět posouzení vlivu na ochranu OÚ, bylo by nadbytečné př. zpracování OÚ pro účely sociálního pojištění zaměstnavatelem.

Adaptační zákon

Jmenování pověřence u orgánů veřejné moci a orgánů zřízených zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu („veřejné subjekty“)

- Jedná se o subjekty, blížící se svojí povahou orgánům veřejné moci.

- Jmenují DPO - notáři a exekutoři, ČNB, NKÚ, Správa hmotných rezerv, veřejný správce práv, VZP
- Nejmenují DPO - Příspěvkové organizace, pomocné instituce např. zdravotnická nebo pečovatelská zařízení, která neprovádí systematický monitoring subjektů údajů nebo rozsáhlé zpracování OÚ zvláštní kategorie, Národní knihovna, ostatní knihovny, divadla ZP s výjimkou VZP

Adaptační zákon

Akreditace subjektů pro vydání osvědčení

- Dozorový úřad nebo akreditační orgán
- Zákon ustanovil certifikační autoritou akreditační orgán
- Český institut pro akreditaci, o.p.s.
- !!!!!Akreditace je zcela dobrovolná – čl. 43/1 b) GDPR

Adaptační zákon

Novinářské zpracování

- Speciální právní titul pro zpracování OÚ
- Ochrana zdroje a obsahu informací
- Výjimka z informační povinnosti
- Výjimka a suspense z některých práv subjektů údajů

Adaptační zákon

Přestupky a pokuty

- Upuštění od pokuty
  - Upozornit na nedostatky
  - Stanovit dobu k nápravě
- Porušení GDPR
  - Max pokuta pro veřejnoprávní subjekty 10 mil Kč

ÚOOÚ v době účinnosti GDPR

- podle GDPR si má každý členský stát stanovit nezávislý dozorový úřad
- v ČR je dozorovým úřadem ÚOOÚ
- GDPR x adaptační zákon – organizace a činnost úřadu

- ÚOOÚ – role dozorového úřadu je stále stejná – stížnostní a kontrolní agenda
- ÚOOÚ – nově:
  - Data breaches
  - Předchozí konzultace
  - Evidence pověřenců
  - Schvalování kodexů chování

ÚOOÚ v době účinnosti GDPR

Data breaches – ohlašování porušování zabezpečení osobních údajů

- Dle čl. 31 GDPR – povinnost ohlásit rizikové případy porušování zabezpečení OÚ pro práva a svobody FO
- Obsah ohlášení – dle GDPR, minimálně:
  - Popis opatření, které správce přijal nebo navrhl s cílem vyřešit dané porušení zabezpečení OÚ
  - Pravděpodobné důsledky pro subjekt údajů
- ÚOOÚ – vyhodnotí přijatá ohlášení
  - Nezahajuje kontroly a neuděluje sankce
  - Do dnešního dne cca 170 ohlášení, dále řešeno je 15 (ohlášení ze soukromé, ale i veřejné sféry, banality, oznámení bez požadovaných náležitostí)
  - Většina obsahovala oznámení hackerských útoků, ztracených zařízení – často řeší precizní zálohování či šifrování – tj. není nutné ani oznamovat ÚOOÚ, nejedná se o rizikové případy

ÚOOÚ v době účinnosti GDPR

Předchozí konzultace

- Konzultace podle GDPR
- V případech, kdy z posouzení vlivů, které správce provedl, přetrvává i přes přijetí opatření ke zmírnění rizika, vysoké riziko pro práva a svobody subjektu údajů
- Nejde o konzultační či osvětovou činnost ÚOOÚ
- Zatím ÚOOÚ neposkytuje

ÚOOÚ v době účinnosti GDPR

Evidence pověřenců

- Jedná se o evidenci nikoliv registraci (pověřenci jsou evidováni u jednotlivých správců a zpracovatelů, nikoliv samostatně) NEZVEŘEJŇUJE SE
- Smyslem je usnadnit kontakt ÚOOÚ se správcem či zpracovatelem
- Aktuálně ÚOOÚ eviduje pověřence u cca 17 000 správců a zpracovatelů
- Pověřenci interní i externí

ÚOOÚ v době účinnosti GDPR

Schvalování kodexů chování

- Vznik kodexů se předpokládá na sektorové úrovní, např. banky, operátoři
- Aby měl kodex váhu, musí jej schválit autorita – dozorový úřad – ÚOOÚ
- Přihlášení se ke kodexu je možností, deklaruje soulad s GDPR
- Není povinností, jen možností

ÚOOÚ v době účinnosti GDPR

Agenda ÚOOÚ

- stížnostní agenda
- kontrolní agenda

Stížnosti/podněty

- hlavně **stížnosti subjektu údajů – důvodné - nedůvodné**
  - ve stížnosti je závažná věc, kterou je třeba ověřit → kontrola
  - v případech, kdy je porušení doloženo → zahájení správního řízení
  - v méně závažných případech poručení → zaslání informace správci a očekávání, že drobné porušení bude ze strany správce napraveno (stovky takových informací ročně)
  - nedůvodné – sdělení stěžovateli, že bylo odloženo, včetně důvodů odložení

ÚOOÚ v době účinnosti GDPR

Stížnosti/podněty

Co dělat, aby na mě podnět nepřišel?

- dodržovat GDPR
- zejména plnit práva subjektů údajů
- při jakémkoliv kontaktu ze strany subjektů údajů – nalézt řešení!!!!

Nejčastější stížnosti

- kamerové systémy
- výkon práv subjektů údajů = neuspokojení práv subjektů údajů
- telemarketing
- nelegální získávání souhlasů

GDPR, právní rámec

- Nařízení (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (obecné nařízení o ochraně osobních údajů)
- GDPR = General Data Protection Regulation (Obecné nařízení o ochraně osobních důvodů)
- Nařízení je platné od 24.5.2016
- Od 25. května 2018 je plně použitelné (účinné) – bez dalšího je závazné a použitelné
- Ještě bude ePrivacy nebo-li Nařízení o respektování soukromého života a ochrany osobních údajů v elektronických komunikacích
- Čekáme na národní zákon o zpracování osobních údajů

GDPR, právní rámec

- Zákon č. 101/2000 Sb., o ochraně osobních údajů bude nahrazen zákonem o zpracování osobních údajů – půjde aktuálně do Senátu
- Pracovní skupina WP29, nyní Evropský sbor pro ochranu OÚ – vydává stanoviska a doporučení, vykládá GDPR

WP 242 - právo na přenositelnost údajů

WP 243 - pověřenci pro ochranu údajů (DPO)

WP 244 - určení vedoucího dozorového úřadu

WP 248 - posouzení vlivu na ochranu údajů (DPIA)

WP 249 - monitoring zaměstnanců

WP 250 - ohlašování případů porušení zabezpečení osobních údajů

WP 251 - automatizované individuální rozhodování a profilování

WP 253 - uplatňování a stanovení správních pokut

WP 259 - souhlas subjektů údajů

WP 260 - transparentnost zpracování

GDPR, právní rámec

- Struktura GDPR - 173 recitálů, 99 článků, cca 100 stran
  - Preambule a vlastní normativní text
    - Preambule, tzv. recitály - výkladová část. Bez informací z preambule bychom GDPR nerozuměli.
    - Vlastní normativní text GDPR – zákonný text, práva a povinností atd.

GDPR – hlavní změny

- GDPR není revoluce
- GDPR přináší detailnější právní úpravu
- GDPR rozpracovává práva subjektů údajů a přidává nová práva (právo na přenositelnost)
- GDPR přináší nové povinnosti (ohlašování případů porušení zabezpečení OÚ, jmenování pověřence, vedení záznamů o zpracování OÚ)
- GDPR zavádí lhůty k plnění právních povinností (3 dny, měsíc)
- GDPR již nezná registraci u Úřadu pro ochranu osobních údajů
- GDPR zavádí vysoké pokuty v případě porušení

Pojmy

Zpracování osobních údajů

- jakákoliv operace s osobními údaji, např. shromáždění, zaznamenání, uspořádání, strukturování, uložení, pozměnění, vyhledávání, nahlédnutí, použití, šíření, seřazení, výmaz, zničení

Osobní údaj

- jakákoliv informace, která se týká identifikované nebo identifikovatelné fyzické osoby nebo fyzické osoby podnikající, např. jméno, datum narození, bydliště, telefon, e-mail, uživatelské jméno, lokační údaje, síťový identifikátor (IP adresa)

Pojmy

Zvláštní kategorie osobních údajů (dříve citlivé)

- rasový či etnický původ, politické názory, náboženské či filosofické přesvědčení, členství v odborech, geometrické či biometrické údaje, zdravotní stav, sexuální orientace
- Nakládání s fotografiemi a kamerovými záznamy není zpracování zvl. kategorie osobních údajů

Subjekt údajů

- fyzická osoba a fyzická osoba podnikající, které se osobní údaje týkají

Pojmy

Správce

- osoba, která určuje účel a prostředky zpracování

Zpracovatel

- osoba, která zpracovává osobní údaje pro správce na základě jeho pokynů, zpracování se řídí smlouvou (povinné náležitosti čl. 28 GDPR)

Správce může být zároveň i zpracovatelem.

Příjemce

- osoba, které jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli.

GDPR a právní tituly zpracování

Právní tituly zpracování OÚ dle GDPR

- Plnění právní povinnosti
- Plnění smlouvy
- Ochrana životně důležitých zájmů
- Veřejný zájem nebo výkon veřejné moci
- Oprávněný zájem
- Souhlas

Právní titul zpracování

- Zpracování na základě několika právních titulů
- Často jeden právní titul zpracování skončí, další pokračuje
- Pokud neexistuje žádný právní titul zpracování, je třeba zpracování ukončit
- Př. Zákazník – plnění smlouvy, plnění právní povinnosti

Plnění právní povinnosti

- Plnění právní povinnosti
  - povinnost vyplývající z právních předpisů např.dle zákoníku práce, zákona o účetnictví, zákona o soc.či zdrav.pojištění
  - nerozšiřovat si povinnosti nad rámec zákonů, zpracovávat jen minimum dle zákonů
  - personálně-mzdová agenda x souhlas – užití OÚ nad rámec standardu, např. fotografie, zasílání informací o zaměstnancích mateřské společnosti, životopis…..personální spis ……..

Plnění právní povinnosti

- Plnění právní povinnosti
  - Personálně mzdová agenda
    - Rozsah dokumentů

- životopisy – souhlas x likvidace

- výběrové řízení na volnou pozici - likvidace

- uzavření pracovního poměru – právní titul plnění právní povinnosti

- ukončení pracovního poměru – zákon o účetnictví – 5 let (DPH 10 let, zákon o sociálním zabezpečení (mzdové listy) – 30 let

Právní tituly

- Ochrana životně důležitých zájmů
  - za účelem předejití vzniku újmy na životě subjektu údajů nebo jiné fyzické osoby, např. ošetření vážně zraněného, monitorování epidemií

- Veřejný zájem nebo výkon veřejné moci
  - zpracování OÚ orgány veřejné moci, pokud mají tuto povinnost za zákona

Právní tituly

Plnění smlouvy

- Velmi častý právní titul
- Existuje smluvní vztah mezi správcem a subjektem údajů, např. zákaznický vztah, smlouvy mezi developerskou společností a klienty
- Zvážit rozsah osobních údajů
- Zaniká s ukončením smlouvy, resp. reklamační lhůtou

Právní titul - souhlas

- Svobodný, konkrétní, informovaný a jednoznačný projev vůle. Subjekt údajů souhlas poskytuje prohlášením nebo jiným zjevným potvrzením (tzv. aktivní souhlas). Souhlas nemusí být písmený, ale správce ho musí prokázat po celou dobu zpracování.
- Souhlas:
  1. Svobodný a konkrétní souhlas – uzavření smlouvy nesmí být podmíněno udělením souhlasu, souhlas obsahuje informace o správci, případně příjemcům, době z pracování, účelu zpracování, možnosti odvolání
  2. Jednoznačný – jasný pozitivní postup – zaškrtnutí políčka
  3. Informovaný – SÚ musí být před udělením souhlasu informovaný o všech skutečnostich zpracovávání dle čl. 13-14 a o svých právech čl. 15-22
  - Odlišitelnost souhlasu – souhlas musí být oddělený od smlouvy, VOP či jiného textu

Právní titul - souhlas

Odvolatelnost souhlasu – subjekt údajů může souhlas kdykoliv odvolat, a to stejně snadně, jako ho udělil

Pro marketing – SOUHLAS

Možnosti získání souhlasu:

- Prostřednictvím online formuláře
- Fyzicky v písemné formě na papíře
- Ústně prostřednictvím telefonu

Souhlas je třeba po celou dobu zpracování prokázat.
Způsoby prokázání:

- Písemný souhlas - uchovat papír s datem a podpisem
- Popsat proces získání souhlasu, evidovat záznam v databázi, včetně datového razítka

Souhlas je třeba po celou dobu prokázat.

Právní titul - souhlas

Zaškrtnutím níže uvedeného okénka „poskytuji souhlas“ udělujete souhlas společnosti .....,IČ:..... ke zpracování:
jména ……..
□ e-mailové adresy …….
□ telefonu …….
□ k marketingovým účelům, tzn. k nabízení produktů
□ k užití osobních údajů společností……. k marketingovým účelům, tzn. k nabízení produktů po dobu 3 let. Tento souhlas můžete kdykoliv odvolat na e-mailu..... S ohledem na zpracování osobních údajů máte práva v souladu s čl. 15 – 22 Obecného nařízení o ochraně osobních údajů 2016/679, zejména právo na přístup k osobním údajům, právo na opravu, právo na výmaz, právo na omezení zpracování, právo na přenositelnost údajů, právo na přenositelnost údajů. Více na www…….cz/nakládání s osobními údaji.

✓ Poskytuji souhlas

Přechod souhlasu

- předpoklad přechodu souhlasu – recitál 171 GDPR
- souhlas byl udělen způsobem a v souladu s GDPR
- souhlas nebyl udělen způsoběm a v souladu s GDPR – dodatečné shojení nebo likvidace
- GDPR neumožňuje využívat OÚ, získané pasivním souhlasem, podmíněným souhlasem, souhlasem v rámci VOP nebo nákupem databází x DLE GDPR POUZE AKTNIVNÍ SOUHLAS

GDPR v marketingové praxi

- Zákon č. 480/2004 Sb., o některých službách informační společnosti, tzv. antispamový zákon - §7
- Šíření obchodních sdělení elektronickými prostředky
  - po předchozím souhlasu
  - zákaznický vztah – souhlas se předpokládá
  - Obsah OS – zřetelné označení, uvedení odesílatele, uvedení možnosti souhlas odvolat

- Očima GDPR
  - Marketing
    - oprávněný zájem – současně existuje zákaznický vztah
    - souhlas
  - Připravuje se Nařízení ePrivacy – bude také přímo účinné

Oprávněný zájem

- jeden z nejflexibilnějších právních důvodů – reciál 47 GDPR
- pro využití tohoto právního titulu by měl existovat relevantní a odpovídající vztah mezi subjektem údajů a správcem, např. zákazník správce x nikoliv vztah nadřazenosti – orgány veřejné moci
- zda subjekt údajů může zpracování OÚ důvodně očekávat
- před zpracováním OÚ na základě tohoto důvodu je třeba provést balanční test = zvážit, zda nad zájmem správce nepřeváží práva subjektu údajů
- výsledek balančního testu je třeba zaznamenat do dokumentu
- např.zpracování osobních údajů pro účely přímého marketingu, ochrana majetku (kamery)

Praktický dopad GDPR do praxe

- Informační povinnost subjektu údajů – čl. 13,14
- Oznámení bezpečnostních incident – čl. 31
- Vhodná technická a organizační opatření na půdě správců, zpracovatelů
- Zásada odpovědnosti správce – velmi posílana

Praktický dopad GDPR do praxe

- Informační povinnost subjektu údajů – čl. 13,14
  - Právo na přístup, opravu, výmaz, omezení zpracování, přenositelnost údajů a právo na námitku – čl. 15 – 22 – viz práva subjektu údajů
- Správce má povinnost v okamžiku získání osobních údajů subjekt údajů informovat o:
  - Správci
  - Údajích, jaké budou zpracovávány
  - Účelu a době zpracování (zda se jedná o poskytnutí OÚ dobrovolně či povinně)
  - Příjemcích OÚ – další správci, nikoliv zpracovatelé
  - Úmyslu předávat OÚ třetích zemí
  - Právech subjektu údajů
- Informace mají být poskytnuty srozumitelně, jednoduše (standardizované ikony), vrstvené informace, ideální formou jsou otázky a odpovědi

Informační povinnost

- Proveditelnost poskytnutí informační povinnosti
  - Zaměstnanci – informační dokument, který podepíší při nástupu, stávající zaměstnanci dopodepsat
  - Dodavatelé – informace ve smlouvách
  - Odběratelé – odkaz na webové stránky, kde budou informace o zpracování osobních údajů zveřejněny

  - Neplnění informační povinnosti je často předmětem stížností!!!!!!
  - DOPORUČENÍ ÚOOÚ – vždy se subjektem údajů komunikovat, domluvit řešení jeho nespokojenosti….

Oznámení bezpečnostních incidentů

- Oznamování incidentů (případů porušení zabezpečení) Úřadu
  - povinné u jakéhokoliv rizikového porušení, a to bez zbytečného odkladu (72 hod)
  - neplatí jen je-li nepravděpodobné riziko pro práva a svobody subjektů (typicky při nemožnosti identifikace subjektů), oznámení by vyžadovalo nepřiměřené úsilí
  - obsahem je popis incidentu, rozsahu, rizik a přijatých opatření – POTŘEBNÝ OBSAH
- Oznamování incidentů subjektům
  - povinné při pravděpodobném vysokém riziku pro práva a svobody
  - opět bez zbytečného odkladu (bez uvedení lhůty)
  - není nutné, pokud byla přijata opatření, kterými nehrozí pro SÚ riziko, např. hesla, šifrování

Oznámení bezpečnostního incidentu

Úřad pro ochranu osobních údajů

Vážení,

v souladu s čl. 33 Obecného nařízení informujeme o incidentu bezpečnosti dat, který znamená ohrožení.

Dne …….. došlo k ……[celkový popis incidentu].

Ohrožená data zahrnují osobní údaje jako například…….. [identifikujte typy ohrožených údajů].

Ohrožená data budou pravděpodobně …… [zveřejněna na Internetu apod.], což může subjektům údajů způsobit tyto důsledky……

Přijali jsem tato opatření…… s cílem vyřešit dané porušení zabezpečení osobních údajů.

Pro další podrobnosti případně kontaktujte našeho pověřence osobních údajů emailem …….. [email] nebo na telefonu .....[telefonní číslo].

V …….dne…… ……..

Vhodná technická a organizační opatření, zabezpečení OÚ

- Správce má povinnost zavést vhodná technická a organizační opatření, aby **zajistil a byl schopen doložit, že zpracovává OÚ v souladu s GDPR**
  - Dodržováním schválených kodexů
  - Uděleným osvědčením
  - Svými vnitřními předpisy – vnitřní předpis o nakládání s osobními údaji

Vhodná technická a organizační opatření, zabezpečení OÚ

- **<u>Zabezpečení osobních údajů</u>**
  - Posouzení rizik pro SÚ, posouzení stavu techniky a rozsahu a účelu zpracování TOMU ODPOVÍDAJÍCÍ ZABEZPEČENÍ
  - Zabezpečení elektronické x faktické (papírové OÚ) – uklízení OÚ, uzamykatelné skříně, zamykání kanceláří, SW přizpůsoben GDPR
  - Např. Pseudonymizace, šifrování, omezení přístupů, přístupová hesla…..

Zásada odpovědnosti

- Správce je povinnen zajistit dodržování GDPR a musí to být schopen prokázat/doložit
- Povinnosti správce

  Zejména:

  - Zavedení vhodných technických a organizačních opatření
  - Vedení záznamů o činnosti zpracování
  - Smluvní zabezpečení vztahu správce – zpracovatel – smlouva o zpracování osobních údajů
  - Ohlašováni bezpečnostních incidentů
  - Provedení posouzení vlivu na ochranu OÚ a předchozí konzultace

Smlouva o zpracování osobních údajů

- Smluvní vztah správce a zpracovatele je v GDPR upravený podrobněji
- Správce je odpovědný za zpracovatele. Má si vybírat jen takové subjekty, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby zpracování bylo v souladu s GDPR (kvalita zpracovatele!!!)
- Obsah smlouvy čl. 28 odst. 3 – předmět, doba trvání zpracování, povaha a účel zpracování, typ OÚ, povinnosti a práva správce ……
- Smlouva – formy smlouvy
- Stávající smlouvy – nahradit novými, dodatky…
- Řetězení zpracovatelů – je stále možné, vždy se souhlasem správce a smluvním zakotvením

Záznamy o činnostech zpracování

- Každý správce (zpracovatel) vede záznamy o činnostech zpracování – čl. 30 GDPR
- Obsah záznamů je podobný jako nynější registrace na ÚOOÚ
- Konkrétně mají záznamy obsahovat:
  - specifikace správce a případně i pověřence
  - účely zpracování
  - popis kategorie subjektu údajů a kategorií osobních údajů
  - kategorie příjemců
  - informace o případném předání údajů do třetí země (+ záruky)
  - plánované lhůty pro výmaz jednotlivých kategorií údajů
  - obecný popis technických a organizačních bezpečnostních opatření
- Záznamy se vyhotovují písemně nebo elektornicky
- Na vyžádání se poskytnou ÚOOÚ

Záznam o činnostech zpracování pro nejmenší podnikatele

jméno a **kontaktní údaje** správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů	*název a kontaktní údaje na svou firmu (na sebe)*
účely zpracování	*důvody, proč zpracovává osobní údaje (nabízení služeb bývalým zákazníkům, kontakt na objednatele služby apod.)*
popis kategorií subjektů údajů	*či osobní údaje zpracovává (zákazníci, zaměstnanci, dodavatelé atd.)*
popis kategorií osobních údajů	*jaké osobní údaje zpracovává (jméno a příjmení, bydliště, číslo mobilního telefonu, e-mailová adresa apod.)*
kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích	*příjemce údajů (osoba, které jsou údaje předávány)*
informace o případném **předání osobních údajů do třetí země** nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk	*při zpracování prováděném nejmenšími podnikateli a živnostníky by k předávání do třetích zemí zpravidla nemělo docházet*
je-li to možné, plánované **lhůty pro výmaz** jednotlivých kategorií údajů	*předpokládaný čas výmazu údajů (po 3 letech od zakázky apod.)*
je-li to možné, **obecný popis technických a organizačních bezpečnostních opatření** uvedených v čl. 32 odst. 1.	*např. uzamčená skříň pro listinné dokumenty, přístupová práva* *k počítači, v němž jsou osobní údaje uloženy*

Práva subjektu údajů

Subjekt údajů

Identifikovaná nebo identifikovatelná žijící fyzická osoba, zejména

- zákazníci (současní, bývalí, potenciální)
- zaměstnanci (současní, bývalí), uchazeči o zaměstnání
- dodavatelé (současní, bývalí, potenciální)
- další osoby (rodinní příslušníci zaměstnanců, návštěvníci
- budovy, veřejnost)

Práva subjektu údajů

Čl. 15-22 GDPR

- došlo k rozšíření stávajícího katalogu práv SÚ
  - Právo na informace o zpracování osobních údajů
  - Právo na přístup SÚ k OÚ
    - Právo získat od správce OÚ potvrzení o zpracování OÚ
    - Právo získat kopie zpracovaných OÚ
  - Právo na opravu
  - Právo na výmaz (právo být zapomenut)
  - Právo na omezení zpracování
  - Právo na přenositelnost OÚ
  - Právo vznést námitku v případě, že zpracování provádí správce na základě svých oprávněných zájmů

Právo na informace

Informační povinnost – čl. 13 a 14 GDPR

- povinnost správce poskytovat informace a sdělení subjektům údajů stručným, transparentním a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků
- informace se lze poskytnout písemně, v elektronické formě a v některých případech i ústně
- ideální forma jsou otázky a odpovědi
- v elektronické podobě na webu

Právo na informace

Informační povinnost – čl. 13 GDPR

- OÚ přímo od subjektů údajů – informační povinnost nejpozději v okamžiku získání OÚ
- Obsah informační povinnosti:
  - totožnost a kontaktní údaje správce a jeho případného zástupce
  - případně kontaktní údaje pověřence pro ochranu osobních údajů
  - účely zpracování a právní základ pro zpracování
  - případné příjemce nebo kategorie příjemců osobních údajů
  - případnýúmyslsprávcepředatosobníúdajedotřetízeměnebo mezinárodní organizaci
  - doba po kterou budou osobní údaje uloženy
  - informace o právech subjektu údajů
  - informace o povinnosti/dobrovolnosti poskytnutí osobních údajů
  - informace o tom, že dochází k automatizovanému rozhodování, včetně profilování

Právo na informace

Informační povinnost – čl. 14 GDPR

- OÚ nejsou od subjektů údajů
- správce je povinen poskytnout informace nejpozději do 1 měsíce od získání osobních údajů nebo v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů nebo při prvním zpřístupnění osobních údajů příjemci (mohou být doplněny standardizovanými ikonami)
- Obsah informační povinnosti je shodný

Právo na přístup k OÚ

- Právo na přístup k OÚ – čl. 15 - přístup SÚ do SW

  - Právo na potvrzení, zda správce OÚ zpracovává, odpověď musí být kvalifikovaná dle čl.15/1
    - účely zpracování, kategorie osobních údajů, kategorie příjemců, plánovaná doba uložení, existence práva na opravu, výmaz, omezení zpracování a právo námitky a stížnosti, informace o zdroji údajů a skutečnost, že dochází k automatizovanému rozhodování; případně na informace o předávání dat mimo EU
  - Právo na kopie zpracovaných OÚ – další kopie mohou být za poplatek

  - Žádosti subjektů údajů musí být bez odkladu vyřízeny, max. do 1 měsíce (max. se dá prodloužit o další 2 měsíce – o tomto prodloužení je nutné informovat)

Právo na opravu OÚ

- povinnost správce opravit bez zbytečného odkladu nepřesné osobní údaje
- povinnost správce doplnit neúplné osobní údaje (s přihlédnutím k účelům zpracování)

Právo na výmaz

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny
- subjekt údajů odvolá souhlas
- subjekt údajů vznese námitky
- osobní údaje byly zpracovány protiprávně
- osobní údaje musí být vymazány ke splnění právní povinnosti

Právo na přenositelnost údajů

- subjekt údajů má právo získat osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci:
  - zpracování je založeno na souhlasu nebo smlouvě
  - zpracování se provádí automatizovaně

  Pokyny Evropského sboru pro ochranu osobních údajů

Právo vznést námitku

- při zpracováńí osobních údajů pro splněńí úkolu prováděného ve veřejném zájmu, při výkonu veřejné moci, nebo pro účely oprávněných zájmů správce nebo třetí strany
  - správce musí prokázat závažné oprávněné důvody pro zpracováńí nebo pro určeńí, výkon nebo obhajobu právních nároků
- při zpracováńí pro účely přímého marketingu (včetně profilováńí)

Subjekt údajů musí být na toto právo výslovně upozorněn (informace musí být uvedena odděleně od jiných informací)

Pověřenec pro ochranu osobních údajů

- Pověřenec – DPO - Data Protection Office
- DPO:
  - dohlíží na dodržování GDPR
  - poskytuje školení a poradenství
  - spolupracuje s ÚOOÚ
  - je kontaktním místem pro subjekty údajů
- DPO se jmenuje v případech:
  - Zpracování OÚ orgány veřejné moci, vyjma soudů
  - Hlavní činnost správce/zpracovatele zahrnuje rozsáhlé, systematické a pravidelné monitorování subjektů
  - Hlavní činnost správce/zpracovatele zahrnuje rozsáhlé zpracování zvláštní kategorie OÚ

Pověřenec pro ochranu osobních údajů

- Pověřenec
  - interní – zaměstnanec
  - externí – na základě smlouvy o poskytování služeb

- Postavení DPO
  - Profesní kvality
  - Nezávislost
  - Zákaz sankcí za výkon funkce
  - Podléhá přímo nejvyššímu vedení
  - Zapojení do všech záležitostí spojených s ochranou OÚ
  - Povinnost mlčenlivosti
  - Zákaz střetu zájmů

Úřad pro ochranu osobních údajů, pokuty

Koordinace postupů jednotlivých úřadů států EU – Evropský sbor pro ochranu osobních údajů

Pokuty

- Až do výše 20 mil. EURO nebo do 4 % celosvětového ročního obratu x dle zákona o zpracování osobních údajů 10 MIO Kč pro veřejné subjekty
- Možné nefinanční postihy – upozornění, napomenutí, zákaz nakládání s OÚ

Praktické tipy pro dodržování GDPR – jak se na GDPR připravit

- analýza aktuálního nakládání s OÚ
  - analýza stávajících databází OÚ, rozsahu OÚ
  - analýza účelů zpracování OÚ
  - analýza přístupu k databázím a zabezpečení OÚ
  - analýza vnitřních předpisů ohledně OÚ

Praktické tipy pro dodržování GDPR – jak se na GDPR připravit

- Příprava potřebných dokumentů
  - Záznamy o činnostech zpracování
  - Informační povinnost pro zaměstnance, spolupracovníky, zákazníky
  - Smlouvy o zpracování osobních údajů
  - Reakce na žádosti subjektu údajů
  - Ohlašování bezpečnostních incidentů
  - Vnitřní předpis o zpracování OÚ

AK SM &Co.
ADVOKÁTNÍ KANCELÁŘ
ŠEBELOVÁ MARIE

FORUM
Naše znalosti pro Váš úspěch

Děkuji za pozornost!

marie.sebelova@aksn.cz, tel:777343639

www.aksn.cz

Tento seminář pořádá

Nakladatelství FORUM s.r.o., divize školení a vzdělávání

Střelničná 1861/8a, Praha 8

tel: +420 251 115 576

fax: +420 251 512 422

office@forum-media.cz

www.forum-media.cz