GDPR

Mgr. Miroslav Galvas,
advokát

2015 právnická firma roku
VELMI DOPORUČOVANÁ KANCELÁŘ

2016 právnická firma roku
VELMI DOPORUČOVANÁ KANCELÁŘ

2017 právnická firma roku
VELMI DOPORUČOVANÁ KANCELÁŘ

ARROWS
advisory group

PROGRAM:

1) Obecné informace a základní pojmy
2) Práva a povinnosti ve vztahu k pokutám
3) Obecná i konkrétní doporučení
4) Diskuze s dotazy

GDPR - POJEM:

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).

- nový právní rámec ochrany osobních údajů v evropském prostoru
- od 25. května 2018 bude přímo stanovovat pravidla pro zpracování osobních údajů

- nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů + nutno pamatovat na zákon o službách informační společnosti

Anglická zkratka Obecného nařízení, se kterou se lze setkat v odborných textech či během přednášky, je GDPR (General Data Protection Regulation).

GDPR – ZÁKLADNÍ POJMY – čl. 4:

OSOBNÍ ÚDAJ:

veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“);

identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například:

- jméno (ale i přezdívka v interním systému, jméno nemusí být celé)
- identifikační číslo (zákazník, živnostník s IČO)
- lokační údaje,
- síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby

- Osobním údajem je i fotografie osoby!

GDPR – ZÁKLADNÍ POJMY – čl. 4:

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**

GDPR – ZÁKLADNÍ POJMY – čl. 4:

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

- Ten, kdo určuje účel zpracování
- Ten, kdo stanovuje prostředky zpracování
- Základní povinnosti dle čl. 5., 6. 12. – 22. GDPR

GDPR – ZÁKLADNÍ POJMY – čl. 4:

ZPRACOVATEL

fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který **zpracovává osobní údaje pro správce**.

- Ten, kdo fakticky prování zpracování a zároveň není správcem (odlišnost osob)
- Dle čl. 29 GDPR nejde o zaměstnance správce!
- Typicky grafik, účetní, advokát atd.
- Základní právní rámec mezi správcem a zpracovatelem určuje čl. 28 odst. 3 GDPR

GDPR – ZÁKLADNÍ POJMY – čl. 4:

- **Souhlas** – svobodný, konkrétní, informovaný, jednoznačný, kdykoliv prokazatelný
- **Dozorový orgán – Úřad pro ochranu osobních údajů**, v každém členském státě určen či vytvořen 1 takovýto úřad (čl. 51 GDPR)
- **Zvláštní kategorie osobních údajů** – údaje o rase, etnickém původu, politických názorech, náboženství, filozofické přesvědčení, členství v odborech, genetické údaje, biometrické údaje, údaje o zdravotním stavu, sexuálním životu a orientaci (čl. 9 GDPR)

REKORDNÍ POKUTY:

5/2017 - Úřad pro ochranu osobních údajů udělil společnosti EURYDIKAPOL, s. r. o. (dříve společnost JH HOLDING s. r. o.) rekordní pokutu ve výši 4.250.000 Kč za šíření nevyžádaných obchodních sdělení.

- společnost neprokázala, že disponovala souhlasy ve smyslu § 7 odst. 2 zákona č. 480/2004 Sb.

- společnost tudíž zasílala nevyžádaná obchodní sdělení bez těchto souhlasů, čímž se dopustila správního deliktu dle § 11 odst. 1 písm. a) bodu 1. citovaného zákona, neboť adresáti nebyli ani jejími zákazníky.

- společnost škodlivou činnost neukončila ani po zahájení řízení

- Maximální možná pokuta 10.000.000,- Kč

MAILINGOVÉ KAMPANĚ:

„Odpovědnost nese kromě samotného rozesílatele ten, v jehož prospěch bylo obchodní sdělení zasíláno, a který takovou rozesílku (mailingovou kampaň) ve svůj prospěch inicioval, a to na základě pokynu, příkazu, uzavřením smlouvy, či jiným obdobným úkonem“

https://www.uoou.cz/zakon-c-480-2004-sb-o-nekterych-sluzbach-informacni-spolecnosti/ds-1497/p1=1497

GDPR – KOHO SE TÝKÁ:

A) Netýká se pouze fyzických osob

B) Týká se v ostatních případech všech právnických osob, kdy některé právnické osoby mají výjimky z některých částí:

- podniky do 250 lidí
  - nemusí mít pověřence (ale riziko pro osobní údaje)
  - nemusí vést záznamy o činnostech zpracování (ale čl. 30 odst. 5)

C) Veřejná správa při výkonu veř. činnosti:

- mají navíc adaptační zákon
- ne příspěvkové organizace (pověřenec – viz dále).

ARROWS advisory group

2015 právnická firma roku
2016 právnická firma roku
2017 právnická firma roku

JAK TO MÍT 100 % SPRÁVNĚ?

Kodexy - mají správcům, zejména na sektorové úrovni, sloužit jako vodítko správné praxe při zpracování osobních údajů právě s ohledem na specifičnost daného sektoru. Kodexy budou moci vydávat sdružení či jiné subjekty zastupující různé kategorie správců nebo zpracovatelů přičemž návrh kodexu musí být předložen Úřadu pro ochranu osobních údajů, který vydá stanovisko, zdali je daný kodex, či návrh na jeho změnu, v souladu s Obecným nařízením a pokud shledá, že ano, schválí jej. Schváleným kodexem se pak můžou řídit správci v daném sektoru, např. bankovnictví či zdravotnictvím.

Osvědčení - má sloužit k prokázání souladu zpracování s Obecným nařízením. Osvědčení o souladu zpracování bude moci vydávat k tomu akreditovaný subjekt. V současné době probíhají práce na stanovení formy a postupů pro akreditaci a pro vydávání osvědčení ze strany akreditovaných subjektů.

Český institut pro akreditaci, o.p.s.

GDPR VS ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ

- GDPR je přímo aplikovatelné (a také velmi podobné)

- Od 25. 5. 2018 bude:
  - nařízení
  - adaptační zákon

- https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5

Tento zákon je pro veřejnoprávní subjekty – horní hranice je limitována

ARROWS advisory group

2015 právnická firma roku
2016 právnická firma roku
2017 právnická firma roku

GDPR – KDY SE (NE)APLIKUJE:

- trestní vyšetřování – viz kompetenční zákon
- zpracování fyzickými osobami
- zpracování anonymních údajů – údaj, který neumožňuje identifikovat osobu (např. statistika) x pozor na pseudonymizaci!

GDPR – POKUTY (a hlavně za co) – čl. 83:

20.000.000 EUR, PODNIK AŽ 4 % Z CELKOVÉHO ROČNÍHO OBRATU:

1) čl. 11 - zpracování a uchovávání dodatečných údajů nutných k identifikaci anonymizovaných a neoznámení subjektu údajů

2) čl.25 (+ čl. 32) **- nezavedení prostředků a vhodných technických opatření** pro zpracování pro provádění zásad ochrany údajů, tzn.:

- zpracovávat opravdu jen nutné údaje
- minimalizace zpracovávaných údajů
- evidence způsobu a množství zpracování, primárně:
  - *množství shromážděných osobních údajů,*
  - *rozsahu jejich zpracování*
  - *doby jejich uložení a jejich dostupnosti*

Opatření zejména zajistí, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.

ARROWS advisory group

2015 právnická firma roku 2016 právnická firma roku 2017 právnická firma roku

GDPR – POKUTY (a hlavně za co) – čl. 83:

20.000.000 EUR, PODNIK AŽ 4 % Z CELKOVÉHO ROČNÍHO OBRATU:

S přihlédnutím ke stavu techniky, **nákladům na provedení**, povaze, rozsahu, kontextu a účelům zpracování **i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob**, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, **případně včetně:**

- pseudonymizace a šifrování
- schopnosti zajistit neustálou důvěrnost, integritu a odolnost systémů
- schopnost obnovy systému v případě poruchy
- PRAVIDELNÉHO TESTOVÁNÍ A POSUZOVÁNÍ RIZIK

V budoucnu dodržování kodexů chování.

Čl. 25 – konkrétní tipy pro ochranu osobních údajů:

1) Ne vždy se jedná o software
2) Úvodní analýza
3) Vnitřní směrnice
4) Ustanovení odpovědné osoby
5) Úvodní školení a průběžné školení
6) Stanovení časového rámce kontrol a doplňování
7) Kontrolování informovanosti
8) Pro nové zaměstnance udělat „Welcome map“
9) V interním systému zavést sledování kroků

JE POVINNÉ ŠIFROVÁNÍ?

Stanovení povinnosti správce a zpracovatele zabezpečit osobní údaje, se obecné nařízení výslovně dovolává ohledu **na stav techniky, náklady na přijetí** a provedení jednotlivých technických a organizačních opatření k zabezpečení osobních údajů.

Šifrování je uvedeno **jako jedno z vhodných opatření** („případně včetně /…/ šifrování osobních údajů“).

Při posuzování úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, jako náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění osobních údajů a neoprávněný přístup k takovým údajům.

GDPR – POKUTY (a hlavně za co):

10.000.000 EUR, PODNIK AŽ 2 % Z CELKOVÉHO ROČNÍHO OBRATU:

1) čl. 26 - společní správci se nedohodnou na míře podílů na odpovědnosti za zpracování u každého z nich pro případ problému
2) čl. 27 - nestanovení společného správce v Unii pro mimounijní
3) čl. 28 - spolupráce s vhodnými zpracovateli

ARROWS advisory group

2015 právnická firma roku
2016 právnická firma roku
2017 právnická firma roku

GDPR – POKUTY (a hlavně za co) – čl. 83:

20.000.000 EUR, PODNIK AŽ 4 % Z CELKOVÉHO ROČNÍHO OBRATU:

čl. 5 - porušení zásad zpracování:

1) Pouze na **základě zákona a korektně (souhlas viz dále)**
2) Účelové omezení – **pouze pro výslovně vyjádřené účely !!!**
3) Pouze v omezeném rozsahu (co **např. životopisy uchazečů?)**
4) Aktualizované údaje a možnost opravy **(indikátory)**
5) Uložit pouze po jasně vymezenou dobu **(směrnice)**
6) Způsob

+ kompatibilní účely (tzn. z plnění smlouvy na vymáhání)

GDPR – POKUTY (a hlavně za co) – čl. 83:

20.000.000 EUR, PODNIK AŽ 4 % Z CELOSVĚTOVÉHO OBRATU:

čl. 6 – zákonnost zpracování – RUŠÍ SE NAHLAŠOVACÍ POV.

Nestabilní – lze kdykoli odvolat	Dodávka Jednorázový nákup	Advokát
SOUHLAS	PLNĚNÍ SMLOUVY	PRÁVNÍ POVINNOST
OCHRANA ŽIVOTNĚ DŮLEŽITÝCH ZÁJMŮ	VEŘEJNÝ ZÁJEM + VÝKON VEŘEJNÉ MOCI	OPRÁVNĚNÝ ZÁJEM
	Vzdělávání	Black out na vrátnici

ARROWS advisory group

2015 právnická firma roku
2016 právnická firma roku
2017 právnická firma roku

GDPR – POKUTY (a hlavně za co) – čl. 83:

20.000.000 EUR, PODNIK AŽ 4 % Z CELOSVĚTOVÉHO OBRATU:

čl. 12 - porušení zásad transparentnosti:

Správce je povinen srozumitelně a jasně splnit informační povinnosti o:

- rozsahu zpracování (kontaktní údaje správce, jaké údaje, apod. – viz. čl. 13)
- práva na opravu
- práva na výmaz

JAK?

- cedule
- subpage
- interní oběžník
- mailové sdělení

ARROWS advisory group

GDPR – POKUTY (a hlavně za co) – čl. 83:

20.000.000 EUR, PODNIK AŽ 4 % Z CELOSVĚTOVÉHO OBRATU:

čl. 15 - právo na přístup (zjistit, co jak a v jakém rozsahu se zpracovává)
čl. 16 - právo na opravu (pokud špatně, musím opravit)
čl. 17 - právo na výmaz (právo být zapomenut)
čl. 18 - povinnost informace o opravě údaje
čl. 22 - zákaz profilovat zákazníky bez souhlasu

GDPR – POKUTY – jak se určí výše?

Při ukládání pokuty se hodnotí (čl. 83/2):

1) Povaha a závažnost (pochybení celého podniku X pochybení oddělení)
2) Úmysl X nedbalost
3) **Kroky učiněné správcem ke zmírnění škod ! (interní vyšetřování, nové směrnice)**
4) **Míra zabezpečovacích opatření (čl. 25 a čl. 32)**
5) Recidiva
6) Míra spolupráce s úřadem
7) Kategorie údajů
8) Osoba se sama přizná, že pochybila X podnět zvenku
9) Dodržování kodexů chování nebo osvědčení
10) Další přitěžující a polehčující okolnosti

Jak by měl vypadat souhlas:

1) Už není nutné uvádět dobu
2) Souhlas musí být svobodný (ne předem vyplněná políčka, nesmí bránit smlouvě) (čl. 4/11)
3) Musí být ale přesně vyjádřen účel (čl. 6/1/a)
4) Souhlas musím být schopen zpětně doložit !
5) Je nutné mít možnost souhlas kdykoli odvolat stejným způsobem, jakým byl udělen (složitost procesu)

Práva:

článek 13 a 14 (poučení):
- znát totožnost a kontaktní údaje správce/zpracovatele/pověřence
- stanovení účelu, doby a právního základu zpracování
- informace ohledně předání
- právo na stížnost, námitku
- právo na odvolání souhlasu
- zdroj původu osobních údajů pokud nejsou získány od subjektu)

článek 15 (právo na přístup a vysvětlení):
- potvrzení od správce, právo na informace viz poučení

článek 16 (právo na opravu):
- bez zbytečného odkladu

článek 18 (právo na omezení zpracování):
- popření přesnosti, protiprávnost zpracování, nepotřebnost, vznesená námitka

článek 21 (právo vznést námitku):
- při vznesení námitky nelze údaje zpracovávat (týká se pouze některých právních základů viz čl. 6)

GDPR – ZÁKAZ EVIDENCE:

Zakazuje se evidovat (**čl. 9**):
- rasu, etnický původ
- přesvědčení, příslušnost k náboženství
- členství v odborech
- genetické a biometrické údaje (biometrické montérky)
- sexuální orientaci

PLATÍ VÝJIMKY:
1) **VÝSLOVNÝ souhlas**
2) **Zpracování je NEZBYTNÉ PRO PLNĚNÍ PRÁVNÍ POVINNOSTI (pracovní právo)**
3) **Zpracování je NEZBYTNÉ PRO ŽIVOTNĚ DŮLEŽITÉ ZÁJMY SUBJEKTU**
4) **ZVEŘEJNĚNÍ SUBJEKTEM**
5) **Další výjimky pro veřejnoprávní orgány atp.**

MAILINGOVÉ KAMPANĚ:

- souhlas musím být udělen přímo ke konkrétní kampani
- nelze používat zakoupené databáze
    - UOOU udělil pokutu ve výši 36 000,- Kč společnosti Zaplo Finance s.r.o., kde zdrojem k rozesílání nevyžádaných obchodních sdělení byla právě zakoupená databáze od třetí společnosti. (Důvodem udělení sankce na spodní hranici je skutečnost, že Úřad obdržel jen málo stížností, a tedy v tomto případě vyhodnotil míru škodlivosti jako relativně nízkou. ÚOOÚ se nicméně bude v rámci prováděných kontrol tímto tématem nadále intenzivně zabývat.)

Společnosti, které využívají či k využití poskytují některé z mnoha databází kontaktů lidí či společností, deklarují, že odpovídají požadavkům vyplývajícím ze zákona. Subjekty, které jsou v těchto databázích uvedeny, jsou proto také často adresáty obchodních sdělení.

Vzhledem k náležitostem, které musí souhlas mít , aby na jeho základě bylo možné legálně zasílat obchodní sdělení třetích stran, považuje ÚOOÚ za nezbytné zdůraznit, že je vysoce nepravděpodobné, že bude existovat taková databáze, jejímž obsahem budou kontakty na osoby, které řádný souhlas udělily. Úřad také upozorňuje na to, že vzhledem k výše uvedenému není možné jako informovaný souhlas posoudit souhlas, který je dán „generálně“, tj. neurčitému okruhu subjektů (šiřitelů) k neurčitým nabídkám.

MAILINGOVÉ KAMPANĚ:

„Odpovědnost nese kromě samotného rozesílatele ten, v jehož prospěch bylo obchodní sdělení zasíláno, a který takovou rozesílku (mailingovou kampaň) ve svůj prospěch inicioval, a to na základě pokynu, příkazu, uzavřením smlouvy, či jiným obdobným úkonem,“ upřesnil mluvčí ÚOOÚ Tomáš Paták.

Dle názoru Úřadu tento závěr vyplývá z § 11 zákona č. 480/2004 Sb., který staví na objektivní odpovědnosti. Smyslem zákona je mj. chránit soukromí adresátů v co nejširší možné míře. Proto je nutné za toho, kdo šíří obchodní sdělení, považovat i takovou osobu, která k šíření obchodních sdělení ve svůj prospěch udělila pokyn, příkaz, uzavřela za tím účelem smlouvu, či provedla jiný, obdobný úkon.

ZVEŘEJNĚNÍ FOTOGRAFIÍ NA WEBU

Častým jevem mnoha firem je zveřejnění fotografií zaměstnanců, vedení, nebo zákazníků či třetích osob účastnících se akcí pořádaných Správcem.

Podmínky zveřejnění:

1. **Účel a právní základ** – smluvní povinnost x souhlas x zákonná licence
2. **Doba zveřejnění**
3. **Způsob zveřejnění**
4. **Odvolání souhlasu/právo být zapomenut**

GENERÁLNÍ SOUHLAS?

Souhlas fyzické osoby, jejíž osobní údaje hodlá správce zpracovávat, je klíčovým institutem evropského modelu ochrany osobních údajů od samých počátků, nelze jej však uplatňovat tam, kde platí jiné právní tituly zpracování (s nimiž nelze souhlas zaměňovat), **např. sjednávání a plnění smluv, plnění povinností či ochrana práv a právem chráněných zájmů.**

Ve srovnání se současným stavem v České republice přináší GDPR formální změnu v tom, že souhlas je rovnocenný pěti dalším právním důvodům/titulům. Jedním ze základních projevů toho je, že souhlas se zpracováním se skutečně uplatní jen tam, kde mohou být naplněny jeho základní znaky, totiž svobodnost a informovanost.

GENERÁLNÍ SOUHLAS?

Případné paušální získávání souhlasu subjektu údajů pro veškerá zpracování, která správce bude provádět k různým účelům, by tak bylo v rozporu hned s několika ustanoveními obecného nařízení, počínaje povinností shromažďovat osobní údaje **pro určité, výslovně vyjádřené a legitimní účely,** přes zásadu transparentnosti vůči subjektu údajů a konče svobodností souhlasu ve vztahu k smluvním vztahům správce a subjektu údajů.

KDY MUSÍ BÝT POVĚŘENEC?

Povinností, kterou správci obecné nařízení ve vztahu k pověřenci pro ochranu osobních údajů ukládá, je pověřence jmenovat a učinit to na základě profesních kvalit jmenované osoby, zejména na základě jejích odborných znalostí práva a praxe v oblasti ochrany osobních údajů a schopnosti plnit úkoly dále pověřenci uložené samotným obecným nařízením.

Žádná specifická forma ověření nebo prokázání profesních kvalit stanovena není, tedy ani forma externě získaného osvědčení. Obecné nařízení ani nedává prostor k tomu, aby formu ověření kvalit nebo nějaké další parametry kvalifikace a osobní způsobilosti stanovily prováděcím předpisem buď Komise (EU) nebo členský stát. Poté, co je pověřenec správcem nebo zpracovatelem jmenován, musí mu ten, kdo ho jmenoval a u koho pověřenec pro ochranu osobních údajů působí, kromě jiného poskytovat zdroje nezbytné k udržování jeho odborných znalostí.

Je samozřejmé, že u správce, u něhož část zpracování osobních údajů probíhá v režimu ochrany utajovaných informací, musí pověřenec splňovat podmínky stanovené příslušnými právními předpisy.

ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

- Čl. 30 GDPR – „nahrazuje“ ohlašovací povinnost
- obsah
  a) Údaje správce (zpracovatele)
  b) Účely zpracování (kategorie zpracování pro každého správce)
  c) Kategorie subjektů
  d) Kategorie příjemců
  e) Informace o předávání (do třetích zemí)
  f) Lhůty pro výmaz je-li to možné
  g) Obecný popis technických opatření pro zabezpečení
- Výjimky odst. 5:
  - **Podnik s méně než 250 zaměstnanci**
  - Rozsudky v trestních věcech
  - Zvláštní kategorie (citlivé údaje)
- **Výjimka z limitace 250 zaměstnanců**:
  - Pravděpodobné riziko pro práva a svobody subjektů
  - Nejde o příležitostné zpracování

ARROWS advisory group

2015 právnická firma roku
2016 právnická firma roku
2017 právnická firma roku

DUPLICITA DOKUMENTŮ

Osobní údaj je uveden v několika dokumentech

- Různé skartační lhůty (RČ na pracovní smlouvě, evidenčním listu, faktuře)
- Poučení subjektu údajů – čl. 13 GDPR
- Skartace dokumentů a právo na výmaz/zapomenutí

ODPOVĚDNOST ZA PORUŠENÍ GDPR

- **Poškozený** = kdokoliv kdo utrpěl újmu (materiální i nemateriální)
- **Liberace** = prokáží, že žádným způsobem nenesou odpovědnost za událost
- **Solidární odpovědnost** správce a zpracovatele
- **Regres** podle výše podílu za škodu
- Rozhodující orgán – určen dle pravidel příslušnosti soudů jednotlivých národních procesních předpisů

KONTAKT NA ADVOKÁTNÍ KANCELÁŘ

SEMINÁŘ VEDL: Mgr. Miroslav Galvas, advokát
WEB: www.arws.cz

ARROWS
advisory group

2015 právnická firma roku
2016 právnická firma roku
2017 právnická firma roku