

GAP analýza GDPR

Ing., Mgr. Luděk Nezmar, MBA

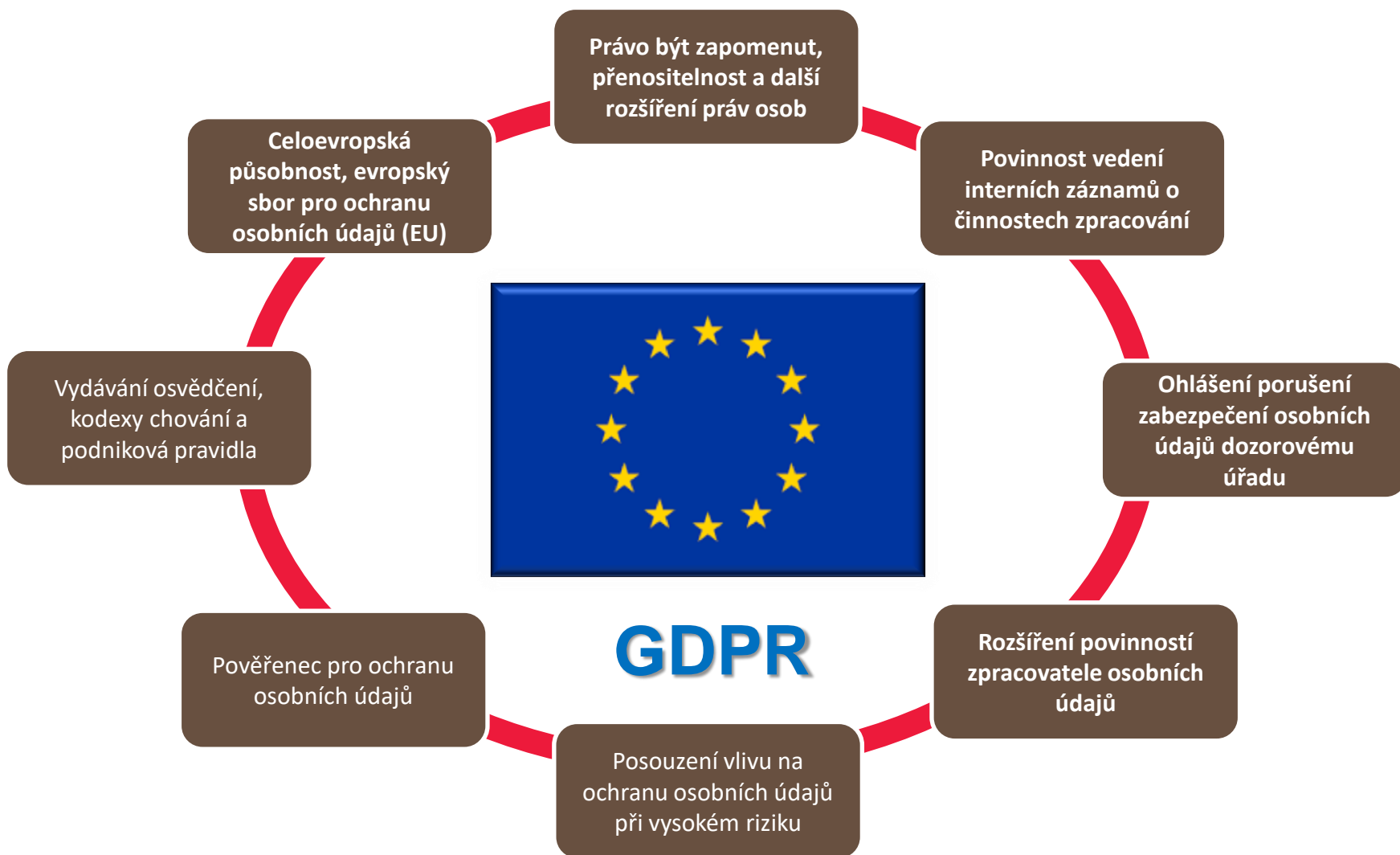
Hotel Olympik, 1. února 2018

GDPR

GAP analýza

- Jak postupovat
- Co hledat
- Kde hledat
- Proč hledat
- Co chtít

Změny v ochraně osobních údajů



Osobní údaj

Jakákoliv informace o fyzické osobě podle níž lze danou osobu **přímo či **nepřímo** identifikovat**

- Jméno
- Pohlaví
- Věk
- Email
- Telefon
- Adresa
- Cookie
- IP adresa
- Fotografie
- Uživatelské jméno...

Zvláštní kategorie osobních údajů

- Rasa nebo etnický původ
- Politické názory
- Náboženství a filozofické přesvědčení
- Členství v odborech
- Genetické a biometrické údaje
- Zdravotní stav
- Sexuální život a orientace

Jak se postavit k požadavkům GDPR?

V první řadě je potřebné upřesnit zpracování ...

- Identifikovat zpracování osobních údajů v organizaci
- K těmto zpracováním určit:
 - Účel zpracování
 - Jaký je právní základ zpracování (souhlas, plnění právní povinnosti, plnění či uzavření smlouvy, oprávněný zájem, veřejný zájem či výkon veřejné moci ...)
 - Kdo je správce a kdo zpracovatel
 - Kde jsou osobní údaje uloženy (manuální, IS)
 - Kdo se v rámci organizace s údaji seznamuje, interní odpovědnost za zpracování
 - Způsob zabezpečení osobních údajů

Cíl identifikace zpracování

- Zjistit **jaká zpracování v organizaci probíhají**
- Určit **interní odpovědnost** za zpracování a ochranu
- Zjištění zda je:
 - zpracování **rizikové**
 - nutné vést **záznamy o zpracování**
 - nutné provést **posouzení vlivu na ochranu osobních údajů** pro konkrétní zpracování
 - nutné zřídit **pověřence pro ochranu osobních údajů**

Na co nezapomenout při identifikaci

- Identifikace zpracování osobních údajů je základní činnost při zahájení implementace GDPR
- Neustále je nutné mít na zřeteli, že **se jedná o ochranu osobních údajů fyzických osob**
- Důležité si **upřesnit zda se opravdu jedná o zpracování osobních údajů**
- V této oblasti odborný orgán může pomoci, ale vždy je třeba **zapojit zástupce organizačních útvarů**, které osobní údaje zpracovávají
- Zpracování osobních údajů **nezužovat na zpracování v informačních systémech**

Formulář k provedení identifikace

IDENTIFIKACE SCÉNÁŘE ZPRACOVÁNÍ

Kontrolní dokument
Dokument ID: GDPR 1 2.2
Počet stran: 3
Název projektu: GAP Analýza
Datum: 6. listopad 2017

- Název scénáře zpracování:
- Krátký popis scénáře zpracování:
(O jaké zpracování se jedná, za jakým účelem je používáno)

IDENTIFIKACE SCÉNÁŘE ZPRACOVÁNÍ

Kontrolní dokument
Dokument ID: GDPR 1 2.2
Počet stran: 3
Název projektu: GAP Analýza
Datum: 6. listopad 2017

| | |
|--|-----------------------------|
| 3. Respondent: (osoba vyplňující tento dotazník) | 4. Vlast (garant) |
| Telefon: | Email |
| Email: | 5. Vlast (správo) |
| Funkce: | Email |

Vymezení vztahu organizace ke zpracování

| | |
|--|--|
| 6. Organizace je v pozici správce: (Pokud ANO, nemůže být i zpracovatelem) Ano / Ne | 7. Orga (Pokud ANO / Ne) |
| 8. Pokud je využíván zpracovatel, existuje smlouva: (Organizace má se zpracovatelem uzavřenu smlouvu o ochraně OÜ) Ano / Ne | 9. Kdo j (Pro kol |
| 10. Je využíván zpracovatel: (Pokud organizace předává data dále ke zpracování) Ano / Ne | 11. Jsou t (Pokud ANO, uveďte u kterého zpracovatele nemá smlouvu) |
| Ano / Ne (Pokud ANO, uveďte u koho se jedná - název firmy apod.) | |

Subjekty údajů

| | |
|--|--------|
| 12. <input type="checkbox"/> Zaměstnanci | Jiné t |
| <input type="checkbox"/> Klienti / zákazníci | |
| <input type="checkbox"/> Pacienti | |
| <input type="checkbox"/> Členi | |
| <input type="checkbox"/> Pachtatelé | |
| <input type="checkbox"/> Osoby do 13 let | |

Právní základ zpracování osobních údajů

| | | |
|---------------------------------------|---|---|
| 13. Identifikátory: | <input type="checkbox"/> Jméno, Příjmení | <input type="checkbox"/> Adresa |
| <input type="checkbox"/> Titul | <input type="checkbox"/> Číslo kreditní karty | <input type="checkbox"/> Místo narození |
| <input type="checkbox"/> Rodné číslo | <input type="checkbox"/> Datum narození | <input type="checkbox"/> Číslo občanského průkazu |
| <input type="checkbox"/> Pohlaví | <input type="checkbox"/> Rodinný stav | <input type="checkbox"/> Číslo cestovního pasu |
| <input type="checkbox"/> Rodinný stav | <input type="checkbox"/> Vzdělání | <input type="checkbox"/> Registrační značka vozu |
| <input type="checkbox"/> Vzdělání | <input type="checkbox"/> Lokality | <input type="checkbox"/> Otitvatský prstů |
| <input type="checkbox"/> Lokality | <input type="checkbox"/> Email | <input type="checkbox"/> Zdravotní dokumentace |
| <input type="checkbox"/> Email | <input type="checkbox"/> Telefon | <input type="checkbox"/> Uživatelské jméno |
| <input type="checkbox"/> Telefon | <input type="checkbox"/> Podobizna | <input type="checkbox"/> Přezdívka |
| <input type="checkbox"/> Podobizna | <input type="checkbox"/> IMEI / UDID | <input type="checkbox"/> Věk |
| <input type="checkbox"/> IMEI / UDID | <input type="checkbox"/> Cookie | |
| <input type="checkbox"/> Cookie | <input type="checkbox"/> IP adresa | |
| <input type="checkbox"/> IP adresa | <input type="checkbox"/> RFID | |
| <input type="checkbox"/> RFID | | |

Právní základ zpracování zvláštních osobních údajů

| | |
|--|--|
| 16. Jedná se o zpracování zvláštních osobních údajů: (Nesjedná se o údaje běžného charakteru) Ano / Ne | 17. Právním (Může být ze |
| 18. Určení kategorie zvláštních údajů (Uvést zda, a v případě, že ano které ze zvláštních kategorií osobních údajů jsou shromažďovány) | <input type="checkbox"/> Udělit <input type="checkbox"/> Plnět <input type="checkbox"/> Oprá |
| <input type="checkbox"/> Rasový / etnický původ | <input type="checkbox"/> Udělit |
| <input type="checkbox"/> Politické názory | <input type="checkbox"/> Plnět |
| <input type="checkbox"/> Náboženské vyznání | <input type="checkbox"/> Oprá |
| <input type="checkbox"/> Filozofické přesvědčení | <input type="checkbox"/> Zprac subj souh |
| <input type="checkbox"/> Členství v odborech | <input type="checkbox"/> Zprac vhod subj |
| <input type="checkbox"/> Genetické údaje | <input type="checkbox"/> Zprac subj |
| <input type="checkbox"/> Biometrické údaje | <input type="checkbox"/> Zprac práv zájm |
| <input type="checkbox"/> Zdravotní stav | <input type="checkbox"/> Zprac prac |
| <input type="checkbox"/> Sexuální život / orientace | <input type="checkbox"/> Zprac oblas |
| | <input type="checkbox"/> Zprac zájm pro s |

IDENTIFIKACE SCÉNÁŘE ZPRACOVÁNÍ

Kontrolní dokument
Dokument ID: GDPR 1 2.2
Počet stran: 3
Název projektu: GAP Analýza
Datum: 6. listopad 2017

| Informování subjektu údajů: | Informace je povinná | Informace byla podána |
|--|----------------------|-----------------------------------|
| 19. /Uvést, zda je pro zpracování povinné provést informaci subjektu údajů, a je-li povinné, zda bylo provedeno/ | Ano / Ne | Ano / Ne |
| Rízení incidentů: | Incident je řízen | Incident by měl být řízen |
| 20. /Uvést, zda je zpracování zahrnuto v současném systému managementu incidentů/ | Ano / Ne | Ano / Ne |
| Uvěst, zda je v rámci zpracování prováděno: | | |
| 21. Profilování | Ano / Ne | 22. Odvozování |
| | | Ano / Ne |
| Použitá technická a organizační opatření: | | |
| 23. Pseudonymizace | Ano / Ne | 24. Generalizace |
| | | Ano / Ne |
| 25. Anonymizace | Ano / Ne | 26. Šifrování |
| | | Ano / Ne |
| Uložení osobních údajů: | | |
| /Uvést, v jakém formátu jsou zpracovávány a ukládány osobní údaje/ | | |
| 27. Listinná podoba | Ano / Ne | 30. |
| 28. Excel, Word, apod. | Ano / Ne | |
| 29. Aplikace nebo IS | Ano / Ne | |
| Doba zpracování: | | |
| /Uvést po jakou dobu je potřebné osobní údaje shromažďovat/ | | |
| 31. Doba uchování | | 32. |
| | | /Uvést normu která dobu stanoví/ |
| Interní odpovědnost za zpracování: | | |
| /Uvést interní odpovědnost za toto zpracování – pozice/ | | |
| 32. | | 33. |
| | | /Uvést email na odpovědnou osobu/ |
| Organizační útvar (y), které se seznamují s osobními údaji: | | |
| 34. | | |
| | | |
| | | |
| | | |
| Poznámky | | |
| 35. | | |

Šablona Identifikace zpracování
Připomínky na info@acresia.com
© ACRESIA Consulting s.r.o.
www.acresia.com

Formulář

Formulář

Šablona Identifikace zpracování
Připomínky na info@acresia.com
© ACRESIA Consulting s.r.o.
www.acresia.com

Šablona Identifikace zpracování v2.1
Připomínky na info@acresia.com
© ACRESIA Consulting s.r.o. 2017
www.acresia.com

Formulář

Klasifikace: 3

Správce a zpracovatel

- **Správce** = osoba určující účel a způsob zpracování osobních údajů
 - Základní odpovědnost za údaje
 - Nové povinnosti
- **Zpracovatel** = zpracovává osobní údaje jménem správce
 - Povinnosti jsou stanoveny nově
 - Sdílená odpovědnost
 - Možnost řetězení zpracovatelů
 - Zpracování osobních údajů

| Vymezení vztahu organizace ke zpracování | |
|---|--|
| 6. Organizace je v pozici správce: (Pokud ANO, nemůže být i zpracovatelem) Ano / Ne | 7. Organizace je v pozici zpracovatele: (Pokud ANO nebúže být i správcem, vzájemně se vylučuje) Ano / Ne |
| 8. Pokud je využíván zpracovatel, existuje smlouva: (Organizace má se zpracovatelem uzavřenu smlouvu o ochraně OÚ) Ano / Ne (Pokud NE, uveďte u kterého zpracovatele nemá smlouvu) | 9. Kdo je správce: (Pro koho jsou údaje zpracovávány - název organizace) |
| 10. Je využíván zpracovatel: (Pokud organizace předává data dále ke zpracování) Ano / Ne (Pokud ANO, uveďte o koho se jedná - název firmy apod.) _____ _____ _____ | 11. Jsou využíváni další subzpracovatelé: Ano / Ne (Pokud ANO, uveďte o koho se jedná - název firmy apod.) _____ _____ _____ |

Subjekt údajů

- **Subjekt údajů** = fyzická osoba, které se údaj týká
 - Zaměstnanci
 - Klienti
 - Pacienti
 - Členi
 - Pachatelé
 - Osoby do 13 let

| Subjekty údajů | | |
|--|--|---|
| 12. <input type="checkbox"/> Zaměstnanci | Jiné typy osob: | |
| <input type="checkbox"/> Klienti / zákazníci | <input type="checkbox"/> Osoba blízká | <input type="checkbox"/> Rodinný příslušník |
| <input type="checkbox"/> Pacienti | <input type="checkbox"/> Zmocněnec | <input type="checkbox"/> Zámce o vzdělávání |
| <input type="checkbox"/> Členi | <input type="checkbox"/> Dodavatel | <input type="checkbox"/> Uchazeč o zaměstnání |
| <input type="checkbox"/> Pachatelé | <input type="checkbox"/> Odběratel | <input type="checkbox"/> Ubytovaná osoba |
| <input type="checkbox"/> Osoby do 13 let | <input type="checkbox"/> Smluvní partner | <input type="checkbox"/> Žadatel, stěžovatel |

Právní základ zpracování (čl. 6 GDPR)

Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

- a) subjekt údajů **udělil souhlas** se zpracováním svých osobních údajů pro jeden či více konkrétních účelů
- b) zpracování je **nezbytné pro splnění smlouvy**, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů
- c) zpracování je **nezbytné pro splnění právní povinnosti**, která se na správce vztahuje
- d) zpracování je **nezbytné pro ochranu životně důležitých zájmů subjektu údajů** nebo jiné fyzické osoby
- e) zpracování je **nezbytné pro splnění úkolu prováděného ve veřejném zájmu** nebo při výkonu veřejné moci, kterým je pověřen správce
- f) zpracování je **nezbytné pro účely oprávněných zájmů příslušného správce** či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě

První pododstavec písm. f) se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů.

Právní základ pro zpracování os. údajů

| | |
|--|-----------------------------------|
| Souhlas | Plnění či uzavření smlouvy |
| Právní povinnost | Oprávněný zájem |
| Veřejný zájem či výkon veřejné moci | Životně důležitý zájem |

Změny v ochraně osobních údajů

- Zákony v oblasti soc. zabezpečení a zaměstnanosti
- Zákon o legalizaci výnosů z trestné činnosti
- Zákon o pojišťovnictví
- Zákon o účetnictví
- Zákon o archivaci
- Zákoník práce
- ...

14. Jedná se o zpracování běžných osobních údajů:

(Nejedná se o údaje zvláštního charakteru)

Ano / Ne

15. Právním základem zpracování je:

(Může být zvolen pouze jeden základ)

- Udělený souhlas
- Plnění smlouvy
- Plnění právní povinnosti
- Ochrana životně důležitých zájmů
- Plnění úkolu ve veřejném zájmu
- Oprávněný zájem

Oprávněný zájem

Nesmí jej v daném případě převážit zájmy nebo základní práva a svobody subjektu údajů

Typicky: **ochrana majetku** (kamerový systém)

Nově také výslovně:

- **Přímý marketing** v mezích legitimního očekávání
- **Předávání ve skupině** pro administrativní účely

Problémy oprávněného zájmu

- Je třeba provést **vyvažování** mezi zájmy správce a subjektu údajů – **balanční analýza**
- Proti zpracování lze **vznést námitku** na základě osobní situace subjektu údajů
- Při námitce je třeba **omezit zpracování** a při vyhovění námitce (negativní výsledek testu přiměřenosti) údaje smazat
- **Široký právní základ, s jistou mírou rizika**

Identifikátory osobních údajů

Osobními údaji jsou **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, 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

| Právní základ zpracování osobních údajů | |
|--|---|
| 13. Identifikátory: | |
| <input type="checkbox"/> Jméno, Příjmení | <input type="checkbox"/> Adresa |
| <input type="checkbox"/> Titul | <input type="checkbox"/> Číslo kreditní karty |
| <input type="checkbox"/> Rodné číslo | <input type="checkbox"/> Místo narození |
| <input type="checkbox"/> Datum narození | <input type="checkbox"/> Číslo občanského průkazu |
| <input type="checkbox"/> Pohlaví | <input type="checkbox"/> Číslo cestovního pasu |
| <input type="checkbox"/> Rodinný stav | <input type="checkbox"/> Registrační značka vozu |
| <input type="checkbox"/> Vzdělání | <input type="checkbox"/> Otisky prstů |
| <input type="checkbox"/> Lokalita | <input type="checkbox"/> Zdravotní dokumentace |
| <input type="checkbox"/> Email | <input type="checkbox"/> Uživatelské jméno |
| <input type="checkbox"/> Telefon | <input type="checkbox"/> Přeždívká |
| <input type="checkbox"/> Podobizna | <input type="checkbox"/> Věk |
| <input type="checkbox"/> IMEI / UDID | |
| <input type="checkbox"/> Cookie | |
| <input type="checkbox"/> IP adresa | |
| <input type="checkbox"/> RFID | |

Zpracování zvláštních kategorií osobních údajů

- Bývalé citlivé údaje dle stávajícího zákona
- **Zakazuje se zpracování osobních údajů**, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby (čl. 9 GDPR)
- Jejich přítomnost signalizuje **vysoká rizika a nutnost vedení záznamů o zpracování**

Právní základ zpracování zvláštních osobních údajů

16. Jedná se o zpracování zvláštních osobních údajů:

(Nejedná se o údaje běžného charakteru)

Ano / Ne

18. Určení kategorie zvláštních údajů

(Uvést zda, a v případě, že ano které ze zvláštních kategorií osobních údajů jsou shromažďovány)

- Rasový / etnický původ
- Politické názory
- Náboženské vyznání
- Filozofické přesvědčení
- Členství v odborech
- Genetické údaje
- Biometrické údaje
- Zdravotní stav
- Sexuální život / orientace

Rozsah a systematicčnost zpracování

Rozsah

Cílem je zjistit zda je zpracování osobních údajů rozsáhlé

Příklad z vodítek skupiny WP29:

- Zpracování – praktický lékař
- **Rozsáhlé zpracování – nemocnice**

Systematické zpracování

Probíhá **pravidelné a stejným způsobem** (dle zavedeného systému)

| | |
|--|--|
| Rozsah zpracování: | |
| <i>(Uvést, kolik subjektů údajů zpracování zahrnuje)</i> | |
| Systematické zpracování: | |
| <i>(Uvést, zda je zpracování systematické)</i> | |

Operace zpracování

- Způsob, jakým je nakládáno s osobními daty
- Slouží k identifikaci, zda se opravdu jedná o zpracování osobních údajů
 - Cloud
 - Uložení dat v diagnostickém přístroji

| Operace zpracování osobních údajů | |
|---|---|
| 19. <input type="checkbox"/> Sběr | Další nespecifikované /Doplňte další případné operace s daty/ |
| <input type="checkbox"/> Uchovávání | |
| <input type="checkbox"/> Validace, kontrola | |
| <input type="checkbox"/> Používání | |
| <input type="checkbox"/> Předávání | |
| <input type="checkbox"/> Nahlížení | |
| <input type="checkbox"/> Archivace | |
| <input type="checkbox"/> Likvidace | |

Informování subjektu údajů

- O zpracování osobních údajů musí být subjekt **transparentně informován**
- Informovat je třeba vždy, pokud již **subjekt informace nemá**
- Informovat nejpozději **do jednoho měsíce** nebo **při první komunikaci či zpřístupnění jinému příjemci**
- **Výjimky** z informování
 - Nemožnost
 - Nepřiměřené úsilí
 - Znemožnění dosažení cílů
 - Zpracování probíhá na základě právní povinnosti a údaje nejsou získány od subjektu údajů
 - Osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství upravenou právem Unie nebo členského státu, včetně zákonné povinnosti mlčenlivosti

Informace a přístup k osobním údajům

- Nový, doplněný obsah informace, která se podává subjektu údajů při převzetí osobních údajů
- Nově se podává i u zpracování k naplnění **právní povinnosti** u případů, kde nabíráte údaje od subjektu údajů
- Obsah informace uveden v článku **13 GDPR**

Informace by se měly podávat i u stávajících zpracování a to minimálně tam, kde je zřízen pověřenec pro ochranu osobních údajů

Článek 13 GDPR

- a) **totožnost a kontaktní údaje správce** a jeho případného zástupce
- b) případně **kontaktní údaje** případného **pověřence pro ochranu osobních údajů**
- c) **účely zpracování**, pro které jsou osobní údaje určeny, a právní základ pro zpracování
- d) **oprávněné zájmy správce nebo třetí strany** v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f)
- e) **případné příjemce nebo kategorie příjemců osobních údajů**
- f) **případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci** nebo, v případech předání uvedených v člancích 46 nebo 47 nebo čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny

Článek 13 GDPR - Pokračování

Je-li to nezbytné pro zajištění spravedlivého a transparentního zpracování:

- a) **doba**, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, **kritéria použitá pro stanovení této doby**
- b) existence **práva** požadovat od správce **přístup k osobním údajům** týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů
- c) pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), **existence práva odvolat kdykoli souhlas**, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním
- d) **existence práva podat stížnost** u dozorového úřadu
- e) skutečnost, **zda poskytování osobních údajů je zákonným či smluvním požadavkem**, nebo požadavkem, který je nutné uvést do smlouvy, a zda má **subjekt údajů povinnost osobní údaje poskytnout**, a ohledně možných důsledků neposkytnutí těchto údajů
- f) skutečnost, že **dochází k automatizovanému rozhodování, včetně profilování**, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů

Použitá technická a organizační opatření

Ověření, zda existuje proces eskalace incidentu

- Zda je proces řízen a existuje
- Zda by měl být řízen

Ověření existence procesu práva nebyt automaticky zpracováván

- Profilování – Například skórování v bance, inzerce na internetu
- Odvozování – Například usouzení na míru schopnosti utrácet peníze

| Řízení incidentů: | | Incident je řízen | Incident by měl být řízen | |
|---|---|-------------------|---------------------------|----------|
| 21. | /Uvést, zda je zpracování zahrnuto v současném systému managementu incidentů/ | Ano / Ne | Ano / Ne | |
| Uvést, zda je v rámci zpracování prováděno: | | | | |
| 22. | Profilování | Ano / Ne | 23. Odvozování | Ano / Ne |

Použitá technická a organizační opatření

Cílem je získat informaci, zda je použité některé z následujících opatření:

- Pseudonymizace
- Šifrování
- Obnova dostupnosti
- Pravidelné testování a hodnocení

Získáváno spíše od odborných orgánů (IT a bezpečnost)

| Použitá technická a organizační opatření: | | | |
|---|----------|----------------------|----------|
| 24. Pseudonymizace | Ano / Ne | 25. Generalizace | Ano / Ne |
| 26. Obnova dostupnosti | | 27. Pravidelné testy | |
| 28. Anonymizace | Ano / Ne | 29. Šifrování | Ano / Ne |

Uložení osobních údajů

Cílem je zjistit v jaké formě jsou osobní údaje zpracovávány s důrazem na automatizování zpracování:

- **Manuální** (včetně Wordu a Excelu)
- IT (**automatizované** – právo na přenositelnost a kritérium pro provádění posouzení vlivu na ochranu osobních údajů)

| Uložení osobních údajů: | | |
|--|----------|---|
| /Uvést, v jakém formátu jsou zpracovávány a ukládány osobní údaje/ | | /Pokud jsou data uložena v systému nebo aplikaci, tak v jaké/ |
| 30. Listinná podoba | Ano / Ne | 31. |
| 32. Excel, Word, apod. | Ano / Ne | |
| 33. Aplikace nebo IS | Ano / Ne | |

Určit dobu zpracování

Cílem je určit dobu, po kterou budou osobní údaje zpracovávány aby tato doba mohla být sdělena subjektu údajů

„Vedle informací uvedených v odstavci 1 poskytne správce subjektu údajů v okamžiku získání osobních údajů tyto další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování:

a) „doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby“ (čl. 13 GDPR)

| Doba zpracování: | |
|---|----------------------------------|
| /Uvést po jakou dobu je potřebné osobní údaje shromažďovat/ | /Uvést normu která dobu stanoví/ |
| 34. Doba uchování | 35. |

Interní účast na zpracování

Cílem je určit kdo interně odpovídá za zpracování (vedoucí útvaru) a ve kterých útvarech, respektive kteří zaměstnanci se zpracování účastní

„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 Unie nebo členského státu.“ (čl. 29 GDPR)

| Interní odpovědnost za zpracování: | |
|--|--|
| /Uvést interní odpovědnost za toto zpracování – pozice/ 36. | /Uvést email na odpovědnou osobu/ 37. |
| Organizační útvar (y), které se seznamují s osobními údaji: | |
| 38. _____ _____ _____ | _____ _____ _____ |

GAP analýza

Cílem prověření stavu je:

- Zjistit jaké nároky na mne GDPR klade
- Identifikovat zpracování osobních údajů
- Provést posouzení rizik pro práva a svobody subjektu údajů
- Jakým způsobem musím doplnit procesy ke zpracování a ochraně osobních údajů včetně procesů posouzení vlivu a ohlašování porušení zabezpečení
- Jak upravit souhlasy a oznámení předávané subjektu údajů
- Jakou vést dokumentaci
- Jak zavést roli Pověřence pro ochranu osobních údajů a další role potřebné (využití stávajících pro zajištění zpracování a ochrany osobních údajů
- Zda bude využito kodexů chování nebo bude absolvován proces získání osvědčení

Analýza rizik zpracování osobních údajů

Posouzení rizik, či jak GDPR definuje „vyhodnocení hrozeb pro práva a svobody fyzických osob“ je možné provést v následujících krocích:

- Určení kritérií analýzy a respondentů
- Návrh a schválení metodiky analýzy rizik
- Identifikace a ohodnocení jednotlivých zpracování
- Identifikace hrozeb
- Vyhodnocení rizik zpracování osobních údajů
- Zpracování, projednání a schválení zprávy o posouzení rizik spojených s jednotlivými zpracováními osobních údajů

Analýza Rizik

GDPR-analýza-rizik aktuální.xlsx - Excel

ACROBAT Řekněte mi, co chcete udělat...

Právítko Řádek vzorců Mřížka Záhloví Lupa 100% Přejít na výběr

Nové okno Uspořádat vše Ukotvit příčky Zobrazit Synchronní posuv Obnovit pozici okna Přepnout okna Makra

K6

| ID_Zpracováni | Scénář | IS | Úroveň dopadu na SÚ (1 - nízký, 5 - vysoký) | Míra IT hrozby (1-nízká, 3 - vysoká) | Míra organizační hrozby (1-nízká, 3 - vysoká) | Finální hodnota rizika | Neoprávněný sběr dat | Neoprávněné použití dat | DPIA ? | id doporučení |
|---------------|---|---------|---|--------------------------------------|---|------------------------|----------------------|-------------------------|----------|---------------|
| Z_1.1 | Správa zákaznických účtů (PVK) | DSM XYZ | 5 | 2 | 3 | 25 | NE | NE | DPIA | |
| Z_1.1 | Správa zákaznických účtů (PVK) | SAP ERP | 5 | 2 | 3 | 25 | NE | NE | DPIA | |
| Z_1.1 | Správa zákaznických účtů (PVK) | Sklad | 5 | 3 | 3 | 30 | NE | NE | DPIA | |
| Z_1.2 | Správa zákaznických účtů (reklamacce) | DSM XYZ | 2 | 2 | 3 | 10 | NE | NE | NOT DPIA | |
| Z_1.2 | Správa zákaznických účtů (reklamacce) | SAP ERP | 2 | 2 | 3 | 10 | NE | NE | NOT DPIA | |
| Z_1.3 | Předsoudní upominání pohledávek (HeG) | Sklad | 5 | 3 | 3 | 30 | NE | NE | DPIA | |
| Z_1.3 | Předsoudní upominání pohledávek (HeG) | DSM XYZ | 5 | 2 | 3 | 25 | NE | NE | DPIA | |
| Z_1.3 | Předsoudní upominání pohledávek (HeG) | SAP ERP | 5 | 2 | 3 | 25 | NE | NE | DPIA | |
| Z_1.3 | Předsoudní upominání pohledávek (HeG) | Sklad | 5 | 3 | 3 | 30 | NE | NE | DPIA | |
| Z_1.3 | Předsoudní upominání pohledávek (HeG) | DSM XYZ | 5 | 2 | 3 | 25 | NE | NE | DPIA | |
| Z_1.3 | Předsoudní upominání pohledávek (HeG) | SAP ERP | 5 | 2 | 3 | 25 | NE | NE | DPIA | |
| Z_1.4 | Předsoudní upominání pohledávek (ZIS) | Sklad | 4 | 3 | 3 | 24 | NE | NE | DPIA | |
| Z_1.4 | Předsoudní upominání pohledávek (ZIS) | DSM XYZ | 4 | 2 | 3 | 20 | NE | NE | DPIA | |
| Z_1.4 | Předsoudní upominání pohledávek (ZIS) | SAP ERP | 4 | 2 | 3 | 20 | NE | NE | DPIA | |
| Z_1.5 | Měření spotřeby/odečty | Sklad | 3 | 3 | 3 | 18 | NE | NE | NOT DPIA | |
| Z_1.5 | Měření spotřeby/odečty | DSM XYZ | 3 | 2 | 3 | 15 | NE | NE | NOT DPIA | |
| Z_1.5 | Měření spotřeby/odečty | SAP ERP | 3 | 2 | 3 | 15 | NE | NE | NOT DPIA | |
| Z_1.5 | Měření spotřeby/odečty | Sklad | 3 | 3 | 3 | 18 | NE | NE | NOT DPIA | |
| Z_1.6 | Soudní vymáhání pohledávek | DSM XYZ | 3 | 2 | 3 | 15 | NE | NE | DPIA | |
| Z_1.6 | Soudní vymáhání pohledávek | SAP ERP | 3 | 2 | 3 | 15 | NE | NE | DPIA | |
| Z_1.6 | Soudní vymáhání pohledávek | Sklad | 3 | 3 | 3 | 18 | NE | NE | DPIA | |
| Z_1.6 | Soudní vymáhání pohledávek | DSM XYZ | 3 | 2 | 3 | 15 | NE | NE | DPIA | |
| Z_1.7 | Přebírání a předávání databázi zákazníků při zaháje | SAP ERP | 2 | 2 | 3 | 10 | NE | NE | NOT DPIA | |
| Z_1.8 | Řešení poruch (balená voda) | Sklad | 3 | 3 | 3 | 18 | NE | NE | NOT DPIA | |
| Z_1.8 | Řešení poruch (balená voda) | DSM XYZ | 3 | 2 | 3 | 15 | NE | NE | NOT DPIA | |
| Z_1.8 | Řešení poruch (balená voda) | SAP ERP | 3 | 2 | 3 | 15 | NE | NE | NOT DPIA | |
| Z_1.9 | Poskytování zvláštních služeb VAK (laboratoř) | Sklad | 3 | 3 | 3 | 18 | NE | NE | DPIA | |
| Z_1.10 | Poskytování zvláštních služeb VAK (laboratoř) | DSM XYZ | 3 | 2 | 3 | 15 | NE | NE | DPIA | |

Připraven

Úvod Metodika Rizika Stupnice Přehled IT Technická opatření Organizační opatření Míra organizačních opatření dopady na SÚ

90%

Posuzování vlivu na ochranu osobních údajů

Obsahem posouzení musí být:

- Popis zamýšlených operací, účelů zpracování a oprávněných zájmů správce
- Zhodnocení nezbytnosti a proporcionality operací ve vztahu k účelům
- Zhodnocení rizika právům a svobodám jednotlivců
- Popis zamýšlených opatření ke zmírnění rizika, včetně bezpečnostních opatření a mechanismů

Pokud riziko zůstává vysoké navzdory přijatým opatřením, je třeba **předchozí konzultace s dozorovým orgánem**

Implementace požadavků GDPR

Implementace probíhá v závislosti na upřesnění z předešlých analýz

Typově se jedná o:

- Realizace **návrhu úpravy/vytvoření procesů** na manipulaci a ochranu osobních údajů včetně jejich zdokumentování
- Spolupráce při úpravě **bezpečnostní architektury IS** zpracovávající osobní údaje
- Podpora nebo **implementace nástrojů** k naplnění požadavků GDPR
- Spolupráce při přípravě **pověřence pro ochranu osobních údajů**
- Spolupráce při provedení **posouzení vlivu** zamýšlených operací zpracování na ochranu osobních údajů
- Příprava na **vydání osvědčení** o ochraně osobních údajů bude-li požadováno

Na co dále nezapomenout

| | |
|--|--|
| Identifikace zpracování | <ul style="list-style-type: none">• Určení účelů a titulů zpracování• Určení podmínek zpracování |
| Pověřenec | <ul style="list-style-type: none">• Vymezit činnosti, nasmlouvat jeho činnost• Vhodné hned po srovnávací analýze |
| Úprava klientských smluv a způsobu informování | <ul style="list-style-type: none">• Úprava klientských smluv, zpracování povinných informací a úprava případného souhlasu |
| Zpracovatelské smlouvy | <ul style="list-style-type: none">• Vymezení nových povinností Správce – Zpracovatel a úprava smluv |
| Posouzení vlivu a systém hlášení | <ul style="list-style-type: none">• Příprava procesu (včetně zdokumentování) pro zpracování posouzení a hlášení |
| Vedení záznamů o zpracování | <ul style="list-style-type: none">• Zdokumentování přijatých technických a organizačních opatření včetně testů a hodnocení |

... je nutné zavedení komplexního systému ochrany a práce s osobními údaji, který je doložitelný

Děkuji za pozornost!

© 2018 Luděk Nezmar, ACRESIA Consulting

Tuto konferenci 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