

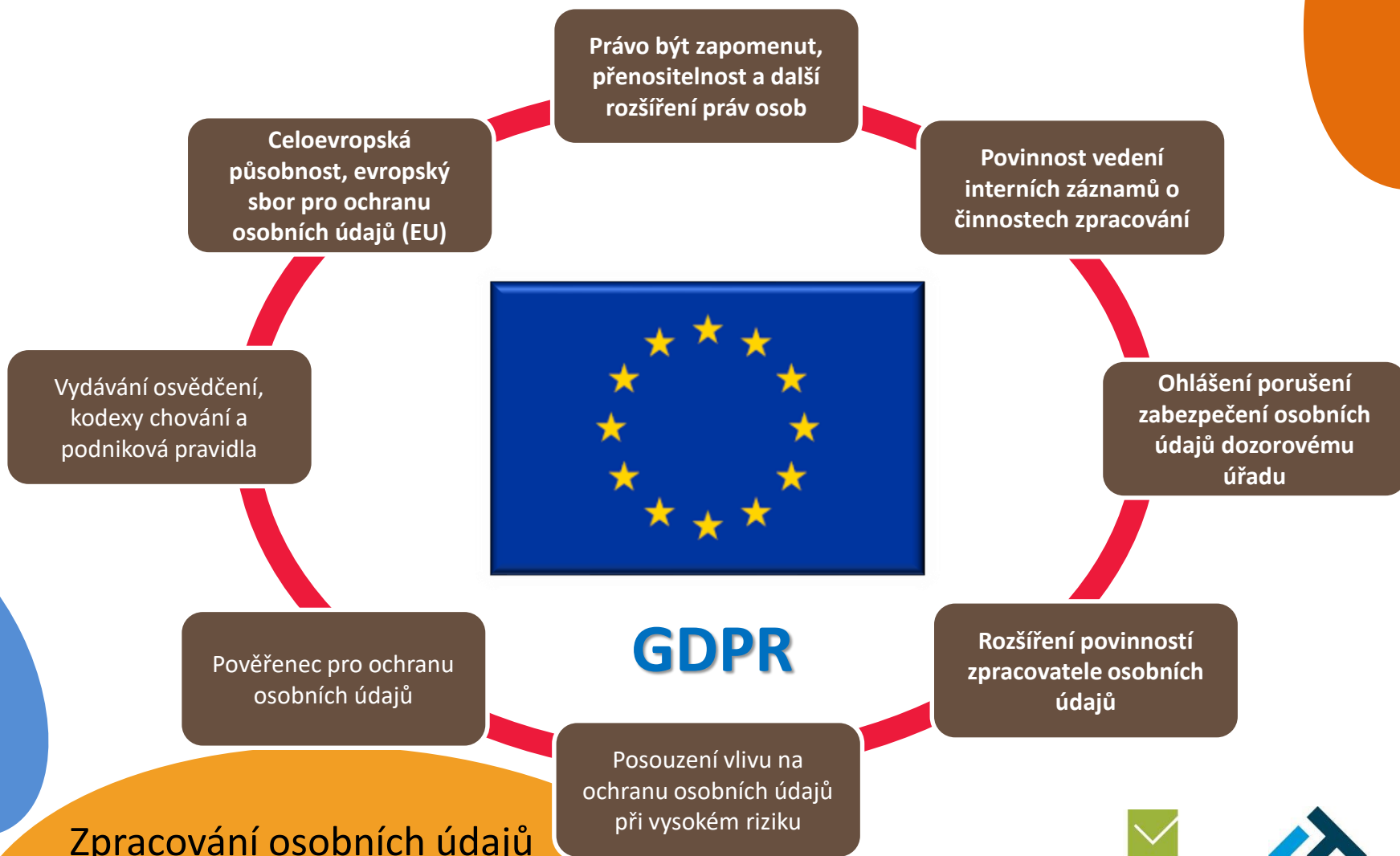
GDPR

Požadavky na dokumentaci

Luděk Nezmar



Změny v ochraně osobních údajů



Zpracování osobních údajů se nemusí registrovat

Obsah dokumentace

- Katalog (registr) zpracování
- Analýza rizik / DPIA
- Posouzení vlivu – DPIA
- Balanční testy proporcionality
- Registr zpracovatelů
- Zpracovatelské smlouvy
- Retenční politika
- Bezpečnostní politika
- Popis pracovního místa Pověřence
- Jmenování Pověřence
- Interní směrnice o ochraně osobních údajů

Obsah dokumentace

- Registr vstupů osobních údajů včetně formulářů
- Účely jednotlivých databází
- Přehled všech evidencí obsahujících osobní údaje
- Vzorek 20 náhodně vybraných subjektů údajů
- Popis způsobu likvidace osobních údajů
- Způsob zajištění aktualizace
- Přehled třetích osob zpracovávajících osobní údaje
- Záznamy o tom, kdo, kdy a co dělal s osobními údaji
- Identifikace zaměstnanců / osob majících přístup k OÚ
- Přehled nápravných opatření

Srovnávací analýza stavu

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

Identifikace zpracování

IDENTIFIKACE SCÉNÁŘE ZPRACOVÁNÍ

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

1. Název scénáře zpracování:

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

3. Respondent:

(osoba vyplňující tento dotazník)

Telefon:

Email:

Funkce:

4. Vlast

(garant)

Email

5. Vlast

(správce)

Email

Vymezení vztahu organizace ke zpracování

6. Organizace je v pozici správce:

(Pokud ANO, nemůže být i zpracovatelem)

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)

10. Je využíván zpracovatel:

(Pokud organizace předává data dále ke zpracování)

Ano / Ne

(Pokud ANO, uveďte o koho se jedná - název firmy apod.)

IDENTIFIKACE SCÉNÁŘE ZPRACOVÁNÍ

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

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"/> Lokality | <input type="checkbox"/> Zdravotní dokumentace |
| <input type="checkbox"/> Email | <input type="checkbox"/> Uživatelské jméno |
| <input type="checkbox"/> Telefon | <input type="checkbox"/> Přezdívka |
| <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 | |

Právní základ zpracování zvláštních osobních údajů

16. Jedná se o zpracování zvláštních osobních údajů:
(Nevědět 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

14. Jedná se

(Nevědět se)

Ano / Ne

15. Právním

(Může být z)

Uděl

Plně

Ochr

Plně

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

Oprá

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:

19. /Uvést, zda je pro zpracování povinné provést informaci subjektu údajů, a je-li povinné, zda bylo provedeno/

Ano / Ne

Ano / Ne

Rízení incidentů:

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/

/Pokud jsou data uložena v systému nebo aplikaci, tak v jaké/

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/

/Uvést normu která dobu stanoví/

31. Doba uchování

32.

Interní odpovědnost za zpracování:

/Uvést interní odpovědnost za toto zpracování – pozice/

/Uvést email na odpovědnou osobu/

32. subj

33.

Organizační útvar (y), které se seznamují s osobními údaji:

34.

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

Formulář

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

Klasifikace: 3

Katalog zpracování

Katalog-zpracování-06-09-2018-ludek - Excel

Základní identifikace		Kategorizace zpracovávaných OÚ		Popis zpracování osobních údajů					Způsob zpracování OÚ				
Oblast zpracování	Název scénáře	ID Zpracování	Účel zpracování	Subjekt OÚ	Kategorie OÚ	Zvláštní kategorie OÚ	Právní titul zpracování	Role	Vlastník scénáře / údajů	Příjemce OÚ	Působnost příjemce	Role příjemce	Základní doba zpracování
Personalistika	CV od uchazečů	1	Získání zaměstnání	Zaměstnanci	Titul Jméno Příjmení Rodné číslo Datum narození Podobizna Jméno manželky	Zdravotní stav	Plnění smlouvy	Správce	Personalista				po dobu trvání pracovního vztahu
Bezpečnost	Kamerový systém	2	Ochrana majetku a zajištění bezpečnosti	Zaměstnanci Klienti / zákazníci Pacienti Návštěvníci	Podobizna		Oprávněný zájem	Zpracovatel	Technik	CAP Cam	EU/EHP	zpracovatel	7 dní

Katalog-zpracování-06-09-2018-l

Vyberte cíl a stiskněte klávesu Enter nebo zvolte příkaz Vložit.

Analýza DPIA

Analýza-DPIA-06-09-2018-ludek - Excel

Identifikační číslo zpracování

Posouzení rizik pro práva a svobody osob pro jednotlivá zpracování

Identifikační číslo zpracování	Úsek / odbor	Název zpracování	Kritéria posouzení																	
			GDPR čl. 35 odst. 3 bod A)	GDPR čl. 35 odst. 3 bod B)	GDPR čl. 35 odst. 3 bod C)	Profilování	Automatické rozhodování	Systematické monitorování	Citlivé údaje	Zpracování je rozsáhlé	Soubory dat porovnány nebo kombinovány	Zahrnutí údajů o zranitelných subjektech	Inovativní tech (biometrika)	Přesun dat i mimo EU	Zpracování zahrnuje výkon práva nebo slu.	Informace o trestních věcech	Proces vyžaduje je DPIA	Právní povinnost správce	Doporučení pro DPIA dle WP29	
1	Personalistika	CV od uchazečů	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ano	Ano	Ano	Ano	Ne	Ne	Ano	Ne	Ano
2	Bezpečnost	Kamerový systém	Ano	Ano	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne

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 – varianta 1

Priloha 5 Mapa rizik v1.04 - Excel

Luděk Nezmar

Soubor Domů Vložení Rozložení stránky Vzorce Data Revize Zobrazení Vývojář Návoděva Rekněte mi, co chcete udělat.

Obecný Normální 2 Normální Neutrální Správně Špatně Kontrolní b...

Vložit Kopírovat Kopírovat formát Schránka Písmo Zarovnáni Číslo Styly Bunky Úpravy

M26 2

ID	Název scénáře zpracování	1				2				3				4				5	
		Zneužití nebo neoprávněná modifikace údajů				Vydávání se za něhko jiného				Neautorizované použití informací				Zneužití systémových zdrojů				Zavedení škodliv	
		Hodnocení		Hodnocení		Hodnocení		Hodnocení		Hodnocení		Hodnocení		Hodnocení		Hodnocení			
Hrozba (H)	Zranitelnost (Z)	Dopad (D)	Významnost (V)	Hrozba (H)	Zranitelnost (Z)	Dopad (D)	Významnost (V)	Hrozba (H)	Zranitelnost (Z)	Dopad (D)	Významnost (V)	Hrozba (H)	Zranitelnost (Z)	Dopad (D)	Významnost (V)	Hrozba (H)	Zranitelnost (Z)		
11	EEN Rešeře z databáze Albertina	1	2	4	8	2	2	4	16	3	2	2	12	1	2	2	4	1	2
12	EEN Firemní rešeře z internetu	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
13	EEN SME Feedback	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
14	EUS_001_vykon kontroly die cl. 23 v programu Interreg V-A CR-Polsko	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
15	EUS_002_vykon kontroly die cl. 23 v programu Interreg Slovensko - Česká republika	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
16	EUS_003_vykon kontroly die cl. 23 v programu spolupráce Česká republika - svobodný stát Bavorsko	1	2	4	8	1	2	4	8	2	3	4	24	1	2	2	4	1	2
17	EUS_004_vykon kontroly die cl. 23 v programu Interreg EUROPE	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
18	EUS_005_vykon kontroly die cl. 23 v programu Interreg CENTRAL EUROPE	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
19	EUS_006_vykon kontroly die cl. 23 v programu Interreg DANUBE	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
20	EUS_007_vykon kontroly die cl. 23 v programu URBACT III	1	2	4	8	3	3	4	36	1	2	2	4	1	2	2	4	1	2
21	EUS_008_vykon kontroly die cl. 23 v programu Interreg V-A Rakousko - Česká republika 2014-2020	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
22	EUS_009_vykon kontroly die cl. 23 v programu spolupráce Svobodný stát Sasko - Česká republika 2014-2020	1	2	4	8	2	4	4	32	1	2	2	4	1	2	2	4	1	2
29	EUS_010_vykon kontroly die cl. 13 v programu Cíl 3 CR-PR - udržitelnost	3	4	4	48	1	2	4	8	1	2	2	4	1	2	2	4	1	2
30	EUS_011_vykon kontroly die cl. 13 v programu Cíl 3 CR-PR - udržitelnost	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
31	EUS_012_vykon kontroly die cl. 13 v programu Cíl 3 BY-CR - udržitelnost	1	2	4	8	3	4	4	48	1	2	2	4	1	2	2	4	1	2
32	EUS_013_vykon kontroly die cl. 13 v programu Cíl 3 Rakousko - CR - udržitelnost	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
33	EUS_014_vykon kontroly die cl. 13 v programu Cíl 3 SA-CR - udržitelnost	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
34	Udržitelnost Integrovaného operačního programu	2	2	4	16	2	2	4	16	2	2	2	8	2	2	2	8	2	2
35	Kontaktní údaje administrátoru	3	2	4	24	3	2	4	24	2	2	2	8	2	2	2	8	2	2
36	Fyzické doklady z udržitelnosti projektu	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
37	Sítznosti IROP	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
38	Proces administrace projektu v MS2014+	2	2	4	16	2	2	4	16	2	2	2	8	2	2	2	8	2	2
39	Evidence přehledu kontrol Vevných zakázek	2	2	4	16	2	2	4	16	2	2	2	8	2	2	2	8	2	2
40	Proces výběrových řízení na Územních odborech	2	2	4	16	2	2	4	16	2	2	2	8	2	2	2	8	2	2
41	Zpracování dotazu k metodice	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
42	Seznam expertů odd. monitoringu	1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
43	Spisová služba	2	2	4	16	1	2	4	8	1	2	4	8	1	2	2	4	1	2
44	e-newsletter Centra pro regionální rozvoj České republiky	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8	1	2
45	Zádosť o informace die z. 106/1999 Sb.	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8	1	2
46	Formulár zpětné vazby "Napište nám"	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8	1	2

Hodnocení Mapa rizik

80%

Identifikace aplikací a opatření

IDENTIFIKACE APLIKACE / SYSTÉMU

Kontrolní dokument
Dokument ID: GDPR I 3.1
Počet stran: 2
Název projektu: GAP Analýza
Datum: 2. listopad 2017

1. **Název aplikace / systému:**

2. **Krátký popis aplikace / systému:**
(k jakému účelu je systém používán)

Základní data aplikace / systému

3. **Respondent:**
(osoba vyplňující tento dotazník)
Telefon:
Email:
Funkce:

4. **Business vlastník:**
(garant dané aplikace)

6. **Aplikace obsahuje osobní údaje:**
(Pokud NE, není nutné dále vyplňovat)
Ano / Ne

8. **Zabezpečení v souladu s politikami:**
(Zabezpečení systému odpovídá platným bezpečnostním organizace)
Ano / Ne

10. **Analýza rizik aplikace / systému:**
(Existuje analýza rizik pro tento systém s ohledem na osobní údaje)
Ano / Ne

GDPR oddíl 2, článek 32, bod 2 - posuzování

11. **Provozní vlastník IT infrastruktury:**
(Společnost u které je aplikace provozována)

13. **Aplikační podpora:**
(Kdo zajišťuje Help Desk - společnost / odpovědná osoba)

GDPR oddíl 2, článek 32, bod 1 a) - pseudonymizace

14. **Aplikace využívá pseudonymizaci OÚ**
(Systém využívá pseudonymizaci osobních údajů)
Ano / Ne

16. **Aplikace využívá šifrování OÚ**
(Systém využívá šifrování osobních údajů)
Ano / Ne

18. **Aplikace využívá generalizaci OÚ**
(Systém využívá generalizaci osobních údajů)
Ano / Ne

IDENTIFIKACE APLIKACE / SYSTÉMU

Kontrolní dokument
Dokument ID: GDPR I 3.1
Počet stran: 2
Název projektu: GAP Analýza
Datum: 2. listopad 2017

GDPR oddíl 2, článek 32, bod 1 b) - zajištění důvěrnosti, integrity, dostupnosti a odolnosti

20. **Aplikace využívá šifrování kanálů**
(Systém využívá šifrování dat šifrovacího spoje)
Ano / Ne

21. **Aplikace využívá k přístupu systém rolí**
(Systém využívá přístupy s určitými úrovněmi pracovních pozic)
Ano / Ne

22. **Aplikace vede auditní systém záznamů**
(Systém vede záznamy všech akcí a manipulací s daty)
Ano / Ne

23. **Aplikace využívá dvou faktorové ověření**
(Systém používá 2 odlišné druhy faktorů (řezavost, vzrušení))
Ano / Ne

24. **Aplikace je sledována v SIEM/SOC**
(Systém je napojen na centrální SIEM/SOC)
Ano / Ne

25. **Aplikace k přístupu využívá FW, VLAN, DMZ**
(Přístup do systému je řízen pomocí FW, VLAN, DMZ)
Ano / Ne

26. **Aplikace je v HA**
(Systém má redundantní nebo repliční)
Ano / Ne

27. **Aplikace je pravidelně zálohována**
(Systém a jeho data jsou pravidelně zálohovány)
Ano / Ne

GDPR oddíl 2, článek 32, bod 1 c) - obnova dostupnosti a přístup u případné incidentu

28. **Aplikace má Disaster recovery plán**
(Systém má Disaster recovery plán)
Ano / Ne

29. **Aplikace má plán zálohování**
(K systému existuje funkční plán zálohování)
Ano / Ne

GDPR oddíl 2, článek 32, bod 1 d) - testování a hodnocení účinnosti opatření

30. **Je prováděn pravidelný test záloh aplikace**
(Zálohy aplikace jsou pravidelně testovány)
Ano / Ne

31. **Incidenty jsou pravidelně vyhodnocovány**
(Je prováděno pravidelné vyhodnocování incidentů)
Ano / Ne

32. **Je prováděn pravidelný test DR scénáře**
(Systém je pravidelně testován na DR scénář)
Ano / Ne

33. **Systém je testován na zranitelnost**
(Je prováděno pravidelné testování zranitelnosti / penetrační testy)
Ano / Ne

GDPR oddíl 2, článek 20, bod 1

34. **Aplikace umožňuje export dat**
(Systém umožňuje export dat)
Ano / Ne

35. **Data z aplikace jsou odesílána mimo systém**
(Data ze systému jsou odesílána)
Ano / Ne

GDPR oddíl 2, článek 13, bod 2 b)

36. **Aplikace umožňuje portabilitu OÚ**
(Systém je připraven na portabilitu OÚ)
Ano / Ne

Poznámky

IDENTIFIKACE OPATŘENÍ

Kontrolní dokument
Dokument ID: GDPR I 3.1
Počet stran: 2
Název projektu: GAP Analýza
Datum: 2. listopad 2017

1. **Respondent:**
(osoba vyplňující tento dotazník)
Telefon:
Email:
Funkce:

2. **Klient:**
(Název organizace)

3. **Projekt:**
(Název projektu)

Existující opatření vztahující se k bezpečnosti osobních údajů

4. **Jsou definovány odpovědnosti za zpracování údajů a související systémy (např. vlastník údajů, vlastník aplikace...):**
Ano / Ne / Pouze pro některé / Pokud pouze pro některé, tak pro které systémy?

5. **Odpovědnosti za zpracování údajů jsou jasné definovány (skupina, holding vs. dceřiné společnosti,**

IDENTIFIKACE OPATŘENÍ

Bezpečnostní opatření

16. **Je využíván princip "Potřeba vědět" pro určení rolí a autorizací:**
Ano / Ne

17. **Přístup k údajům je zajištěn bezpečným procesem autentizace a bezpečnými hesly (např. silná hesla, pravidelné změny hesel)?**
Ano / Ne

18. **Počet privilegovaných účtů a účtů správců je omezen na minimum a pravidelně kontrolován:**
Ano / Ne

19. **Přístup k osobním údajům je možný pouze pomocí konkrétních uživatelských profilů a individuálních identifikátorů uživatelů?**
Ano / Ne

20. **Existuje postup schvalování a zrušení přístupových práv a jsou hesla bezpečně předávána:**
Ano / Ne

21. **Přístupová práva jsou pravidelně kontrolována a aktualizována:**
Ano / Ne

22. **Přístup pro administrativní úlohy k osobním údajům zvláštní kategorie je zabezpečen pokročilými bezpečnostními opatřeními jako např. federated identity, certifikát, 2-faktorové ověřování:**
Ano / Ne

23. **Přístup k zálohám a kopiím dat (zejména karty USA/NOG) je zajištěn pomocí ověřování a šifrování:**
Ano / Ne

24. **Je zaveden koncept fyzické bezpečnosti, který bere v úvahu požadavky na různé zóny zabezpečení (např. veřejné prostory, kancelář, datové centra, oblasti s vysokou mírou bezpečnosti):**
Ano / Ne

25. **Pro přístup do kanceláře je vyžadováno oprávnění fyzického přístupu (např. přístupová karta / klíče pro otevření dveří, kontrola na recepci). Existuje poplašný systém a systém řízení přístupu:**
Ano / Ne

26. **Je přístup do serverových místností a datových center přísně omezen na oprávněné osoby a jsou zavedena pokročilá bezpečnostní opatření (např. PIN kód). Je kdykoli možné určit, které osoby měly**
Ano / Ne

6. **Zaměstnanci jsou školeni v oblasti ochrany osobních údajů a přijata opatření na zvyšování povědomí:**
Ano / Ne

8. **Výběr zpracovatelů a poskytovatelů služeb je omezen na definovaných kritériích výběru a auditu:**

Smlouvy se zpracovatelé zahrnují

10. **Smlouvy zahrnují zajištění zničení dat po skončení zpracování:**
Ano / Ne / Pouze pro některé

12. **Smlouvy zahrnují pravidla pro subdodávky zpracování:**
Ano / Ne / Pouze pro některé

14. **Smlouvy zahrnují právo na audit zpracování údajů:**
Ano / Ne / Pouze pro některé

Analýza rizik – aplikace

1	GDPR								
2	SYSTÉM	Popis	Business vlastník	IT vlastník	Osobní údaje	Citlivé osobní údaje	Pokud obsahuje citlivé osobní údaje, uveďte jaké	Odpovídá zabezpečení systémem platným bezpečnostním politikám společnosti?	Máte analýzu rizik pro tento systém s ohledem na ochranu osobních údajů?
3	Název systému	Krátký popis systému - k čemu se používá	Kontaktní údaje garanta dané aplikace		ANO/NE (Pokud NE, není nutné vyplňovat další sloupce)	ANO/NE (Pokud NE, není nutné vyplňovat další sloupce)	Např.: rozsudky v trestních věcech, zdravotní stav, údaje o dětech aj.	ANO/NE	ANO/NE
4	Váha opatření	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	Athena	Podrobný popis Athény	Neznámý respondent	Neznámý respondent	NE	ANO	Členství v odborech Genetika Rasa a etnicita	ANO	NE
6	Ginis				NE	NE		NE	NE
7	Helios				NE	NE		NE	NE
8	Pohoda				NE	NE		NE	NE
9	SAP				NE	NE		NE	NE

1	GDPR oddíl 2, článek 32, bod 1 a), pseudonymizace a šifrování										GDPR oddíl 2, článek 32, bod 1 b), zajištění neustálé důvěrnosti, integrity,									
2	Provozni vlastník IT infrastruktury	Provozni vlastník aplikace	Aplikační podpora	Využíváte v systému pseudonymizaci OUI/COU?	Využíváte v systému šifrování OUI/COU?	Přístup k systému pouze přes šifrované kanály?	Má systém řízený přístup k OUI/COU dle pracovní pozice uživatelů?	Vedete auditní záznamy k systému?	Používáte dvoufaktorové ověření?	Je systém napojen na SIEM/SOC?										
3	Společnost u které je aplikace provozována	Kdo aplikaci vlastní (společnost, odpovědná osoba)	Kdo zajišťuje Help Desk (společnost / odpovědná osoba)	ANO/NE	ANO/NE	ANO/NE	ANO/NE	ANO/NE	ANO/NE	ANO/NE										
4	N/A	N/A	N/A	1	3	2	2	1	2	2										
5	Česká pošta	Účetní	Cloud	ANO	ANO	ANO	NE	NE	NE	ANO										
6				NE	NE	NE	NE	NE	NE	NE										
7				NE	NE	ANO	ANO	ANO	ANO	ANO										
8				ANO	ANO	ANO	ANO	ANO	ANO	ANO										
9				NE	NE	NE	NE	NE	NE	NE										



Analýza rizik - opatření

A	B	C	D	E	F	G
1	2	3	1	2	3	3
Váha opatření						
Oblast zpracování	Identifikované zpracování	ID_Zpracování	Jsou definovány odpovědnosti za zpracování údajů a související systémy (např. Vlastník údajů, Vlastník aplikace...)?	Jsou odpovědnosti za zpracování údajů jasně definovány? (skupina <-> dceřiné společnosti, vlastníci údajů, zaměstnanci, dodavatelé, společné zpracování atd.).	Jsou zaměstnanci školeni v oblasti ochrany údajů a jsou přijata opatření na zvyšování povědomí?	Existuje definovaný nákupní proces týkající se uzavírání smluv zpracovateli? Je výběr zpracovatelů služeb založen definovaných kritériích výběru a
Bezpečnost	Kamerový systém	Z_2	Ano	Ano	Ano	Ano
Personalistika	CV od uchazečů	Z_1	Ano	Ne	Ne	Ne

O	P	Q	R	S	T
1	3	2	1	1	2
Jsou přístupová práva pravidelně kontrolována a aktualizována?	Je přístup pro administrativní složky k osobním údajům zvláštní kategorie zabezpečeny pokročilými bezpečnostními opatřeními jako např. federated identity, certifikát, 2-faktorové ověřování?	Je zajištěn přístup k zálohám a kopiím dat (zejména karty USB/HDD) pomocí ověřování a šifrování?	Je zaveden koncept fyzické bezpečnosti, který bere v úvahu požadavky na různé zóny zabezpečení (např. veřejné prostory, kancelář, datové centra, oblasti s vysokou mírou bezpečnosti)?	Pro přístup do kanceláře je vyžadováno oprávnění fyzického přístupu (např. přístupová karta / klíče pro otevření dveří, kontrola na recepci)? Existuje poplachový systém a systém řízení přístupu?	Je přístup do serverových místností a datových center přísně omezen na oprávněné osoby a jsou zavedena pokročilá bezpečnostní opatření (např. PIN kód). Je možné určit, které osoby mají přístup kdykoliv?
Ano	Ano	Ano	Ano	Ano	Ano
Ne	Ne	Ne	Ne	Ne	Ne

Analýza rizik – dopady na SÚ

GDPR-analýza-rizik - Excel

Formula: =SVYHLEDAT(\$B8;Organizační opatření!\$B\$4:\$C\$39;2;NEPRAVDA)

ID	Scénář (PVK)	IS	DPIA	Úroveň dopadu na SÚ (1 - nízký, 5 - vysoký)	Dopady na SÚ			
					I.0001 Osobní údaje	I.0002 Datové přenosy	I.0003 Vzdálená správa	I.0004 Původ dat
Z_1.1	Správa zákaznických účtů (PVK)	DSM XYZ	DPIA	5	ANO	ANO	NE	NE
Z_1.1	Správa zákaznických účtů (PVK)	SAP ERP	DPIA	5	ANO	ANO	NE	NE
Z_1.1	Správa zákaznických účtů (PVK)	Sklad	DPIA	5	ANO	ANO	NE	NE
Z_1.2	Správa zákaznických účtů (reklama)	DSM XYZ	NOT DPIA	2	ANO	ANO	NE	NE
Z_1.2	Správa zákaznických účtů (reklama)	SAP ERP	NOT DPIA	2	ANO	ANO	NE	NE
Z_1.3	Předsoudní upomínání pohledávek (HeG)	Sklad	DPIA	5	ANO	ANO	NE	NE
Z_1.3	Předsoudní upomínání pohledávek (HeG)	DSM XYZ	DPIA	5	ANO	ANO	NE	NE
Z_1.3	Předsoudní upomínání pohledávek (HeG)	SAP ERP	DPIA	5	ANO	ANO	NE	NE
Z_1.3	Předsoudní upomínání pohledávek (HeG)	Sklad	DPIA	5	ANO	ANO	NE	NE
Z_1.3	Předsoudní upomínání pohledávek (HeG)	DSM XYZ	DPIA	5	ANO	ANO	NE	NE
Z_1.3	Předsoudní upomínání pohledávek (HeG)	SAP ERP	DPIA	5	ANO	ANO	NE	NE
Z_1.4	Předsoudní upomínání pohledávek (ZIS)	Sklad	DPIA	4	ANO	ANO	NE	NE

Analýza rizik – výsledek

Analýza rizik-06-09-2018-ludek - Excel

ID	Zpracování	Aplikace	Dopad na subjekty údajů	Míra IT hrozby	Míra organizační hrozby	Finální hodnota rizika	Neoprávněný sběr dat	Neoprávněné použití dat	Potřeba provést DPIA	ID doporučení
	procesy zpracování osobních údajů	informační systémy	1 - nízký, 5 - vysoký	1 - nízká, 3 - vysoká	1 - nízká, 3 - vysoká					
Z_1.1	CV od uchazečů	Pohoda	3	2	3	15	Ne	Ano	Ne	
Z_1.2	CV od uchazečů	Helios	4	3	3	24	Ano	Ano	Ano	
Z_2.3	Kamerový systém	SAP	N/A	3	1	N/A	N/A	N/A	Ne	
Z_2.5	Kamerový systém	Athena	N/A	3	1	N/A	N/A	N/A	Ne	

https://www.acresia.com/index.php?option=com_gdpr&view=risk&Itemid=1744

Hledat

Zveřejněno	ID	Zpracování	Aplikace	Úroveň dopadu na SÚ	Míra IT hrozby	Míra organizační hrozby	Finální hodnota rizika	Neoprávněný sběr dat	Neoprávněné použití dat	Potřeba provést DPIA	Doporučení	Actions
<input checked="" type="checkbox"/>	3	CV od uchazečů	Pohoda	3	2	3	15	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	2	CV od uchazečů	Helios	4	3	3	24	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>		Kamerový systém	SAP	N/A	3	1	N/A	<input type="checkbox"/>	<input type="checkbox"/>	N/A		<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>		Kamerový systém	Athena	N/A	3	1	N/A	<input type="checkbox"/>	<input type="checkbox"/>	N/A		<input type="checkbox"/> <input type="checkbox"/>

Zobrazit 5

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**

Registr DPIA

05.2 DPIA Registr CZ - Excel

Je DPIA nezbytné?

A	B	C	D	E	F	G	H	I	J	K	L	
Registr Posouzení vlivu na ochranu osobních údajů (DPIA)												
Úvodní dotazník												
Obsahuje váš produkt, využívá, uchovává nebo	Používá váš produkt nebo služba osobní údaje k předvídání osobních preferencí, umístění,	Pomáhá váš produkt rozhodování, které může významně	Zahrnuje váš produkt nebo služba nějaké systematické	Existují další rizika spojená s								
						Dotazník k posouzení vlivu na ochranu osobních údajů ACRESIA Consulting! Pouze odpověď Ano / Ne. Pokud ano, odpovězte prosím na otázky v části dotazníku o posouzení dopadů ochrany údajů.						
						(Nepovinná otázka) Jaké jsou	(Nepovinná otázka) Uveďte prosím stručné vysvětlení o tom, jak se					
Zpracovávat činnosti												
	(Povinné) Dokážete odhadnout obnůh údajů v rámci vašeho produktu / součástí svého produktu ano, kolik? (Povinné) Zpracováváte v rámci vašeho produktu / služby osobní údaje dětí ve věku do 15 let? (Povinné) Můžete potvrdit shromážděné osobní údaje relevantní a omezují na to nezbytné k jejich shromáždění?											

DPIA-06-09-2018: Ka-nerovny-system-1 [jen pro čtení] - Word

2 Definicce projektu/systému/řešení

2.1 Hlavní

Otázka	Ano	Ne	Nepřístupí	Nejsme si jisti
Bylo DPIA provedeno na předchozí verzi tohoto projektu?		X		
Změnilo se něco od doby, kdy bylo dokončeno poslední DPIA?		X		
Bylo vyhledáno doporučení DPO k provedení tohoto DPIA?		X		

2.1.1 Nový projekt nebo jeho nová verze?

Je toto nový projekt nebo nová verze již existujícího projektu?

Nový projekt	Nová verze	Existující produkt/systém	Nejsme si jisti
		X	

2.1.2 Samostatné nebo v setu

Je toto DPIA adresováno samostatnému zpracování nebo celému setu podobných zpracování, které zůstávají podobně riskové?

Samostatné zpracování	Set podobných zpracování	Nejsme si jisti
	X	

2.1.3 Popis zpracování

Podle GDPR musí všechna DPIA obsahovat „systematický popis předpokládaného zpracování“ (GDPR Art. 35(7)(a)).

Prosíme, vložte váš popis níže:

Klienti poskytují identifikační údaje o společnosti (IČ, DIC, adresa) a o osobě odpovědné za poskytnutí nebo poskytnutí hlasovacího systému (jméno, pozice ve společnosti, e-mail a telefonický kontakt).

Informace o zakoupených certifikátech společnosti jsou pole sdíleny a prezentovány v dalších relevantních oznámeních Rizicové.

Posouzení vlivu na ochranu osobních údajů (DPIA)

Základní informace

Identifikace správce	BWI Czech Republic s.r.o. Mikulášská 226/2, 350 02 Cheb IČ: 04181352 Schránka: q@bwi.cz Email: gdpr@bwi.cz Kontaktní osoba: Jara Nováková
Důvod pro provádění DPIA	Standardní Posouzení pro práva a svobody při zpracování osobních údajů na základě analýzy rizik.

Účel zpracování

Popis účelu zpracování osobních údajů	Ochrana majetku správce a ochrana života a zdraví osob pohybujících se ve sledovaném prostoru pomocí kamerového systému.
Právní základ zpracování	Čl. 6 odst. 1 písm. f) GDPR - zpracování je nezbytné pro účely oprávněných zájmů správce

Rozsah zpracování

Zpracovávané kategorie osobních údajů	Vizualní a přírodní zvukové identifikační údaje ve formě kamerového záznamu.
---------------------------------------	--

Balanční test proporcionality

WALMARK a.s.

Hledat

Zveřejněno	ID	Dokumenty	Oblasti	Přehled zpracování	Účel zpracování	Právní základ	Respondent	Vlastník údajů
<input checked="" type="checkbox"/>	1	Personalistika	CV od uchazečů	Získání zaměstnání	Plnění smlouvy	Neznámý respondent	Účetní IT adm	
<input checked="" type="checkbox"/>	2	Balanční test	Bezpečnost	Kamerový systém	Ochrana majetku a zajištění bezpečnosti	Oprávněný zájem	Neznámý respondent	Technik IT adm

Zobrazit 5

BT 1 - Albertina v1.3 - Word

Balanční test proporcionality produktu Albertina

Souhrnné informace o produktu

ID produktu	1
Název produktu/scénáře	Bisnode Albertina
Název systému	Databáze MS SQL
Krátký popis produktu/scénáře	Díky široké škále údajů a různým výběrovým kritériím Bisnode Albertina pomáhá svým uživatelům najít potenciální zákazníky a minimalizovat náklady na marketingové kampaně tím, že poskytuje nástroj pro přesné cílení. Také umožňuje zákazníkovi analyzovat portfolio klientů, aby našli potenciální klienty, ke kterým by cílili a aby mohli minimalizovat obchodní riziko.
Respondent	Jiří Čech
Telefon Respondent	725 776 298
Email Respondent	jiri.cech@bisnode.com
Funkce Respondent	Product Manager
Business vlastník	Jiří Čech
Email Business vlastník	jiri.cech@bisnode.com
IT vlastník	Jiří Čech
Email IT vlastník	jiri.cech@bisnode.com
Provozní vlastník IT infrastruktury	Master data
Provozní vlastník aplikace	Bisnode, Jiří Škopový
Aplikační podpora	Bisnode, Radka Kosová
Aplikace obsahuje osobní údaje	ANO
Aplikace obsahuje zvláštní osobní údaje	NE

Identifikace oprávněného zájmu

Otázka	Odpověď	Poznámka
1.1 Jaký je účel produktu?	Nástroj pro segmentaci trhu a analytický nástroj pro snížení míry kreditního a úvěrového rizika, ověření solidnosti partnera, důvěryhodnosti společnosti.	První etapa je identifikovat oprávněný zájem - jaký je účel zpracování osobních údajů?

Zpracovatelé

→ ↻ 🏠 https://www.acresia.com/index.php?option=com_gdpr&view=processors&Itemid=1664
Most Visited Getting Started Překladač Google



Hlavní strana

Home > DPO Tools > Zpracovatelé

Hledat



Vyhledat ▾

Zrušit

Zveřejněno	ID	Zpracovatel	Činnost zpracovatele
✓	1	Benefit	Externí účetní firma zpracovávaj
✓	2	LMC	Společnost zajišťující hodnocení
✓	3	Microsoft	Provozovatel cloudových služeb

07.11 Procesní dotazník pro shodu s GDPR - správa - Word

Adresát
k rukám vedení společnosti
Ulice
PSČ Město

V [místo] dne 6. září 2018

INFORMACE O POSTUPU SOUVISEJÍCÍM S ÚPRAVOU SMLUVNÍ DOKUMENTACE

Vážení,

obracíme se na Vás v souvislosti s právním auditem, který naše společnost [název organizace], se sídlem [sídlo organizace], IČ: [IČ organizace] dále jen („Organizace“), v současné době interně vykonává za účelem dosažení souladu s požadavky nařízení Evropského parlamentu a Rady 2016/679, ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů („Nařízení“), které nabýlo účinnosti dne 25. května 2018. Součástí prováděného auditu je i revize smluv a jiných právních ujednání s partnery společnosti Organizace. Tímto dopisem se obracíme na Vás, jakožto na partnera Organizace, s cílem objasnit zamýšlený budoucí postup.

Nařízení neboli „GDPR“ (společně s adaptačním zákonem o zpracování osobních údajů, jehož finální podoba ani den nabytí účinnosti ještě nejsou známy) v České republice nahrazuje současnou právní úpravu ochrany osobních údajů v podobě zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů („ZOOÚ“), který provádí evropskou směrnici 95/46/ES, a tím představí nový právní rámec ochrany osobních údajů v evropském prostoru. Pro Nařízení je typická jeho přímá aplikovatelnost v členských státech Evropské unie, a tudíž se nová úprava dotýká všech společností, institucí i jednotlivců, kteří shromažďují a zpracovávají osobní údaje fyzických osob nacházejících se v Evropské unii, a to neohledně na to, v jaké pozici tyto subjekty s osobními údaji nakládají (zda z pozice správce, zpracovatele, příjemce osobních údajů apod.). Nařízení stanoví mimo jiné nové povinnosti vztahující se na správce a zpracovatele osobních údajů, přičemž nadáčením těchto povinností je nadávením

Ne

Zobrazit 5

Retenční politika

MČ Praha 2 [úroveň klasifikace]

Příloha – Plán uchování dat

Kategorie záznamu osobních údajů	Povinná retenční doba	Vlastník záznamu
Mzdové listy	30 let po ukončení pracovního poměru	Oddělení personalistiky
Smlouvy s dodavateli	Sedm let po skončení smlouvy	Oddělení nákupu

ACRESIA Consulting
Chcete-li tento dokument vyplnit, nejprve si přečtěte zásady uchování údajů.

ACRESIA Consulting
Existují tři možnosti pro definování doby uchování:
a) Povinná doba je uvedena v místní legislativě - např. daňové, pracovní, archivační a podobné zákony.
b) Vymazání může být vyvoláno událostí - např. data zákaznickovi mohou být po odeslání produktu smazána; ihned jak návštěvník opustí web.
c) Pověřenec pro ochranu osobních údajů určí příslušnou dobu uchování údajů

ACRESIA Consulting
Jedná se pouze o příklady. Tuto tabulku vyplňte příslušnými údaji pro vaši organizaci.

Obsah

1. ÚČEL, ROZSAH A UŽIVATELÉ.....
2. REFERENČNÍ DOKUMENTY.....
3. PRAVIDLA UCHOVÁVÁNÍ.....
 - 3.1. OBECNÉ ZÁSADY UCHOVÁVÁNÍ.....
 - 3.2. OBECNÝ PLÁN UCHOVÁVÁNÍ.....
 - 3.3. ZABEZPEČENÍ DAT BĚHEM DOBY UCHOVÁVÁNÍ.....
 - 3.4. LIKVIDACE DAT.....
 - 3.5. PORUŠENÍ, PROSAZOVÁNÍ A DODRŽOVÁNÍ PŘEDPISŮ.....
4. LIKVIDACE DOKUMENTŮ.....
 - 4.1. PRAVIDELNÝ PLÁN LIKVIDACE.....
 - 4.2. METODA LIKVIDACE.....
5. SPRÁVA ZÁZNAMŮ UCHOVÁVANÝCH NA ZÁKLADĚ TOHO.....
6. PLATNOST A SPRÁVA DOKUMENTŮ.....
7. DODATKY.....

Pověřenec - DPO

- Jmenování
- Oznámit úřadu a veřejnosti
- Stanovit kompetence a úkoly
 - Monitorování souladu s legislativou
 - Realizace úkolů spojených s prováděním posouzení vlivu
 - Spolupráce s dozorovým úřadem (ÚOOÚ)
 - Prosazovat přístup založený na riziku
 - Zdokumentovat a dále udržovat přehledy operací zpracování
 - Informovat a radit všem zaměstnancům
 - Spolupracovat při vytvoření systému ochrany OÚ
 - Zajistit možnost školení a povědomí
 - Sledovat dodržování zásad

Registr vstupů osobních údajů

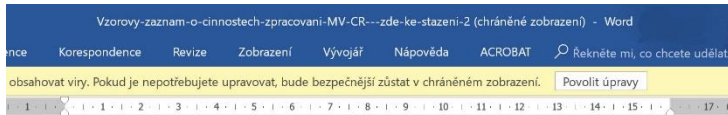
Registr vstupů osobních údajů - Excel

ID	Oblast	Zpracování	Datový vstup	Aplikace / místo	Vlastník aktiva	Informace subjektu údajů podána	Platnost od	Platnost do	Vzor
		procesy zpracování osobních údajů		formuláře / aplikace / url					
Z_1.1	Personalistika	Nástup uchazeče o zaměstnání	Vstupní dotazník	Nástupní dotazník - pdf	vedoucí personalistiky	Ne	01.01.2018	dosud	Ne
Z_2.1	Informatika	Odesláni životopisu přes web	Kontaktní formulář	http://www.firma.cz/zivotopis	Správce webu společnosti	Ano	25.04.2012	25.05.2018	Ano
Z_3.1	Účetnictví	Uplatnění snížení daně	Dotazník na snížení daně	Pohoda	mzdová účetní	N/A	20.06.2016	dosud	N/A

JMÉNO		PŘÍJMENÍ	
Titul před jménem		Titul za jménem	
Rodné příjmení		Dřívější příjmení	
DATUM NAROZENÍ		RODNÉ ČÍSLO	
Zdravotní pojišťovna		ČÍSLO OP	
Stav:		ZPS *	<input type="checkbox"/> ANO <input type="checkbox"/> NE
Pobíráte důchod? *	<input type="checkbox"/> ANO <input type="checkbox"/> NE	Jaký druh důchodu?	
Místo narození		Občanství (pokud jiné než české, uveďte č.pasu)	
Trvalé bydliště	PSC: Ulice:	Město: Čp.:	
Přechodné bydliště	PSC: Ulice:	Město: Čp.:	
Doručovací adresa *	<input type="checkbox"/> Trvalé bydliště <input type="checkbox"/> Přechodné bydliště	<input type="checkbox"/> Jiné, jaké?	
E-mail		Mobilní telefon	
Číslo fidičského oprávnění		Skupiny fidičského oprávnění *	A B C D E T

Rodinní příslušníci			
Partner *	<input type="checkbox"/> Manžel/ka <input type="checkbox"/> Druh/Družka	Jméno	Příjmení
Rodné číslo			
Zaměstnan/a		Bydliště	
Jméno dítěte	Příjmení		Rodné číslo

Záznamy o zpracování



Záznam o činnostech zpracování - VOLBY Čl. 30 odst. 1 obecného nařízení o ochraně osobních údajů (GDPR)	
Správce: ... (název, adresa, datová schránka) ...	
Zástupce správce: ... (jméno, příjmení, funkční zařazení osoby odpovědné za agendu) ...	
Pověřenec pro ochranu osobních údajů: ... (jméno, příjmení, e-mail) ...	
I. Účely zpracování	
ZAJIŠTĚNÍ AGENDY OBCE PODLE VOLEBNÍCH ZÁKONŮ	
Čl. 6 odst. 1 písm. c) GDPR - zpracování nezbytné pro plnění právní povinnosti:	
zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů, zákon č. 130/2000 Sb., o volbách do zastupitelstev krajů a o změně některých zákonů, zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí a o změně některých zákonů, zákon č. 62/2003 Sb., o volbách do Evropského parlamentu a o změně některých zákonů, zákon č. 275/2012 Sb., o volbě prezidenta republiky a o změně některých zákonů (zákon o volbě prezidenta republiky), prováděcí právní předpisy k volebním zákonům.	
II. Kategorie subjektů údajů	
Občan obce – volič. Člen okrskové volební komise. Kandidát. Zmocněnec. Petent.	
III. Kategorie osobních údajů	
Základní identifikační údaje, státní občanství, volební právo a jeho případné omezení, číslo dokladu totožnosti, účast při hlasování; v případě členů okrskových volebních komisí údaje nezbytné pro výkon činnosti člena komise a pro jeho odměňování; v případě kandidátů a zmocněnců identifikační údaje dle kandidátní listiny a čestného prohlášení kandidáta; v případě petentů u nezávislých kandidátů identifikační údaje dle náležitostí petice.	
IV. Kategorie příjemců	
Členové okrskových volebních komisí pro účely plnění jejich povinností podle volebních zákonů. Kontrolní orgány (krajský úřad, Státní volební komise).	
V. Plánované lhůty pro výmaz kategorií osobních údajů	
Platí skartační lhůty stanovené vyhláškami k volebním zákonům: ve vztahu ke kandidátním listinám a souvisejícím dokumentům - A10, pro ostatní volební dokumentaci - V5.	
VI. Obecný popis technických a organizačních bezpečnostních opatření	
Listinná vyhotovení volební dokumentace jsou ukládána v uzamčených prostorách a v průběhu voleb se pečují. Přístup k elektronickým datovým souborům je zabezpečen hesly v souladu s nastavením přístupových práv vnitřními předpisy obce.	

Záznamy správce o činnostech zpracování osobních údajů

podle čl. 30 odst. 1 Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016,

obecného nařízení o ochraně osobních údajů (dále jen „Nařízení“), vedené společností:

Alfa, s. r. o.

se sídlem Horoměřická 12, Praha 2, PSČ 120 00

IČO: 123 45 546

společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C,

vložka 12458

kontaktní emailová adresa: ..., telefonický kontakt: ...

(dále jen „Správce“)

1. Kontaktní údaje pověřence pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů nebyl u Správce jmenován.

2. Popis kategorií subjektů údajů, kategorií osobních údajů a účelů jejich zpracování

a) Zákazníci Správce

Kategorie osobních údajů: Identifikační a kontaktní údaje zákazníků.

Účel zpracování osobních údajů: Uzavření a plnění smlouvy mezi zákazníkem a Správcem, plnění s tím souvisejících zákonných povinností vůči zákazníkům a orgánům veřejné správy.

Právní základ zpracování osobních údajů: Plnění smlouvy a zákonem stanovených povinností, např. v souvislosti s vyřizováním reklamací zákazníků nebo archivací účetních dokladů obsahujících osobní údaje zákazníků.

b) Zaměstnanci Správce

Kategorie osobních údajů: Identifikační a kontaktní údaje zaměstnanců, údaje o bankovním spojení, zdravotním pojištění a sociálním zabezpečení.

Účel zpracování osobních údajů: Uzavření a plnění povinností zaměstnavatele vyplývajících z pracovní smlouvy a obecně závazných právních předpisů.

Právní základ zpracování osobních údajů: Plnění smlouvy a zákonem stanovené povinnosti, např. registrační a oznamovací povinnosti vůči příslušným úřadům.

c) Osoby vstupující do monitorovaných prostor Správce

Kategorie osobních údajů: Obrazové nahrávky bez zvukové stopy.

Účel zpracování osobních údajů: Zajištění ochrany majetku Správce, který se nachází v monitorovaném prostoru.

Právní základ zpracování osobních údajů: Oprávněný zájem Správce (ochrana majetku), zpracování osobních údajů příslušnými úřady.



Další dokumentace

- Účely jednotlivých databází
- Přehled všech evidencí obsahujících osobní údaje
- Vzorek 20 náhodně vybraných subjektů údajů
- Popis způsobu likvidace osobních údajů
- Způsob zajištění aktualizace
- Přehled třetích osob zpracovávajících osobní údaje
- Záznamy o tom, kdo, kdy a co dělal s osobními údaji
- Identifikace zaměstnanců / osob majících přístup k OÚ
- Přehled nápravných opatření

GDPR dokumentace



EU GDPR Složka dokumentace

Poznámka: Dokumentace by měla být ideálně v podobě níže uvedeného seznamu.

Č.	Kód dokumentu	Název dokumentu	Odpovídající články GDPR
1			
Příprava projektu a analýza			
1	1.1	Identifikace zpracování	
2	1.2	Identifikace IT systému	
3	1.3	Identifikace opatření	
4	1.4	Pokyny pro mapování datových a zpracovatelských činností	
2			
Rámec politiky osobních údajů			
5	2.1	Zásady ochrany osobních údajů	Článek 24(2)
6	2.2	Zásady ochrany osobních údajů zaměstnanců - směrnice	Článek 24(2)
7	2.3	Ochrana osobních údajů - web	Články 12, 13 and 1
8	2.4	Registrace oznámení o ochraně osobních údajů	GDPR Články 12, 13 and 14
9	2.5	Zásady uchování dat	Články 5(1)(e), 17, 30
10	2.6	Příloha - Plán uchování dat	Článek 30
11	2.7	Popis pracovního místa pověřence pro ochranu osobních údajů	Články 37, 38, 39
12	2.8	Cookies - prohlášení na web	
13	2.31	Prohlášení o ochraně osobních údajů - web	
14	2.33	Ochrana osobních údajů - web	
15	2.34	Informace o zpracování osobních údajů pro dodavatele	
16	2.51	Plán uchování osobních údajů CZ	
3			
Mapování zpracovatelských činností			
17	3.1	Pokyny pro mapování datových a zpracovatelských činností	Článek 30
18	3.2	Příloha - Katalog (registri) zpracování	Článek 30
19	3.3	Otázky GAP analýza	
4			
Správa práv subjektu údajů			
20	4.1	Formulář souhlasu se zpracováním údajů subjektu	Články 6(1)(a), 7(1), 9(2)



Č.	Kód dokumentu	Název dokumentu	Odpovídající články v GDPR
21	4.2	Formulář pro odejmutí souhlasu se zpracováním údajů subjektu	Článek 7(3)
22	4.3	Formulář rodičovského souhlasu	Článek 8
23	4.4	Formulář pro odejmutí rodičovského souhlasu	Článek 8
24	4.5	Postup žádosti o přístup k údajům subjektu	Články 7(3), 15, 16, 17, 18, 20, 21, 22
25	4.6	Formulář žádosti o přístup k údajům subjektu	GDPR Článek 15
26	4.7	Formulář pro zveřejnění údajů subjektu	GDPR Článek 15
5			
Posouzení dopadů na ochranu OÚ			
27	5.1	Metodika posouzení vlivu na ochranu OÚ	Článek 35
28	5.2	Registr posouzení	Článek 35
29	5.3	Identifikace DPIA	
30	5.4	Balanční test proporcionality	
31	5.5	Posouzení rizik pro práva a svobody osob	
32	5.6	Metodika analýzy rizik	
33	5.7	Analýza rizik z hlediska subjektů údajů	Článek 33
6			
Přenosy osobních dat			
34	6.1	Přehrániční postup pro přenos osobních údajů	Články 1(3), 44, 45, 46, 47, 49
35	6.2	Příloha 1 - Standardní smluvní doložky pro předávání osobních údajů správčům	Článek 46(5)
36	6.3	Příloha 2 - Standardní smluvní doložky pro předávání osobních údajů zpracovatelům	Článek 46(5)
7			
Shoda s třetími stranami			
37	7.1	Procesní dotazník pro shodu s GDPR	GDPR Články 28, 32
38	7.2	Smlouva o zpracování osobních údajů - role správce	Články 28, 32, 82
39	7.3	Smlouva o zpracování osobních údajů - role zpracovatele	Články 28, 32, 82
40	7.4	Příloha ke smlouvě	
41	7.5	Modelové příklady správce - zpracovatel	
8			
Bezpečnost osobních údajů			
42	8.1	Zásady bezpečnosti IT	Článek 32
43	8.2	Pravidla řízení přístupu	Článek 32
44	8.3	Bezpečnostní postupy pro oddělení IT	Článek 32



Č.	Kód dokumentu	Název dokumentu	Odpovídající články v GDPR	Mandatorní povinnost dle GDPR
45	8.4	Zásady BYOD (přineste si vlastní zařízení)	Článek 32	
46	8.5	Zásady užití mobilních zařízení a teleworkingu	Článek 32	
47	8.6	Zásady čistého stolu a obrazovky	Článek 32	
48	8.7	Zásady klasifikace informací	Článek 32	
49	8.8	Zásady anonymizace a pseudonymizace	Článek 32	
50	8.9	Zásady užití kryptování	Článek 32	
51	8.10	Plán obnovy po havárii	Článek 32	
52	8.11	Postup interního auditu	Článek 32	
53	8.12	Dodatek - Kontrolní seznam interního auditu ISO 27001	Článek 32	
54	8.13	Katalog hrozeb a zranitelnosti CZ		
55	8.14	Zápis o kontrole ochrany osobních údajů		
9				
Porušení bezpečnosti osobních údajů				
56	9.1	Postup při odhalení porušení a oznamování	Články 4(12), 33, 34	✓
57	9.2	Registrace porušení bezpečnosti údajů	Článek 33(5)	✓
58	9.3	Oznamovací formulář při porušení bezpečnosti údajů určený úřadu dohledu	Článek 33	✓
59	9.4	Oznamovací formulář porušení bezpečnosti údajů pro subjektů údajů	Článek 34	✓
10				
Ostatní zásady				
60	10.1	Zásady zpracování OÚ v call centru		
61	10.3	Zásady provozování kamerového systému		
10				
Zaměstnanci				
62	11.1	Prohlášení o mlčenlivosti		
63	11.2	Informace pro zaměstnance		
64	11.3	Souhlas zaměstnance		

* Tento dokument je povinný, pokud (a) zpracování provádí veřejný orgán nebo jiný státní orgán, s výjimkou soudů, které jednájí v soudní moci; nebo (b) se hlavní činností právnické osoby skládají ze zpracovatelských operací, které svou povahou, působností a / nebo účely vyžadují ve velkém měřítku pravidelné a systematické sledování subjektů údajů; nebo (c) hlavní činností právnické osoby je zpracování rozsáhlých souborů zvláštních kategorií údajů podle článku 9 GDPR nebo osobní údaje týkající se odsouzení za trestný čin a trestných čin uvedených v článku 10 GDPR.

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

www.acresia.com



ACRESIA
CONSULTING