ACRESIA CONSULTING

FORUM

GDPR

Požadavky kladené na DPO

Luděk Nezmar

Změny v ochraně osobních údajů

GDPR

- **Právo být zapomenut, přenositelnost a další rozšíření práv osob**
- **Povinnost vedení interních záznamů o činnostech zpracování**
- **Ohlášení porušení zabezpečení osobních údajů dozorovému úřadu**
- **Rozšíření povinností zpracovatele osobních údajů**
- Posouzení vlivu na ochranu osobních údajů při vysokém riziku
- Pověřenec pro ochranu osobních údajů
- Vydávání osvědčení, kodexy chování a podniková pravidla
- **Celoevropská působnost, evropský sbor pro ochranu osobních údajů (EU)**

ACRESIA CONSULTING

FORUM

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

ACRESIA CONSULTING

FORUM

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

ACRESIA CONSULTING

FORUM

Srovnávací analýza stavu

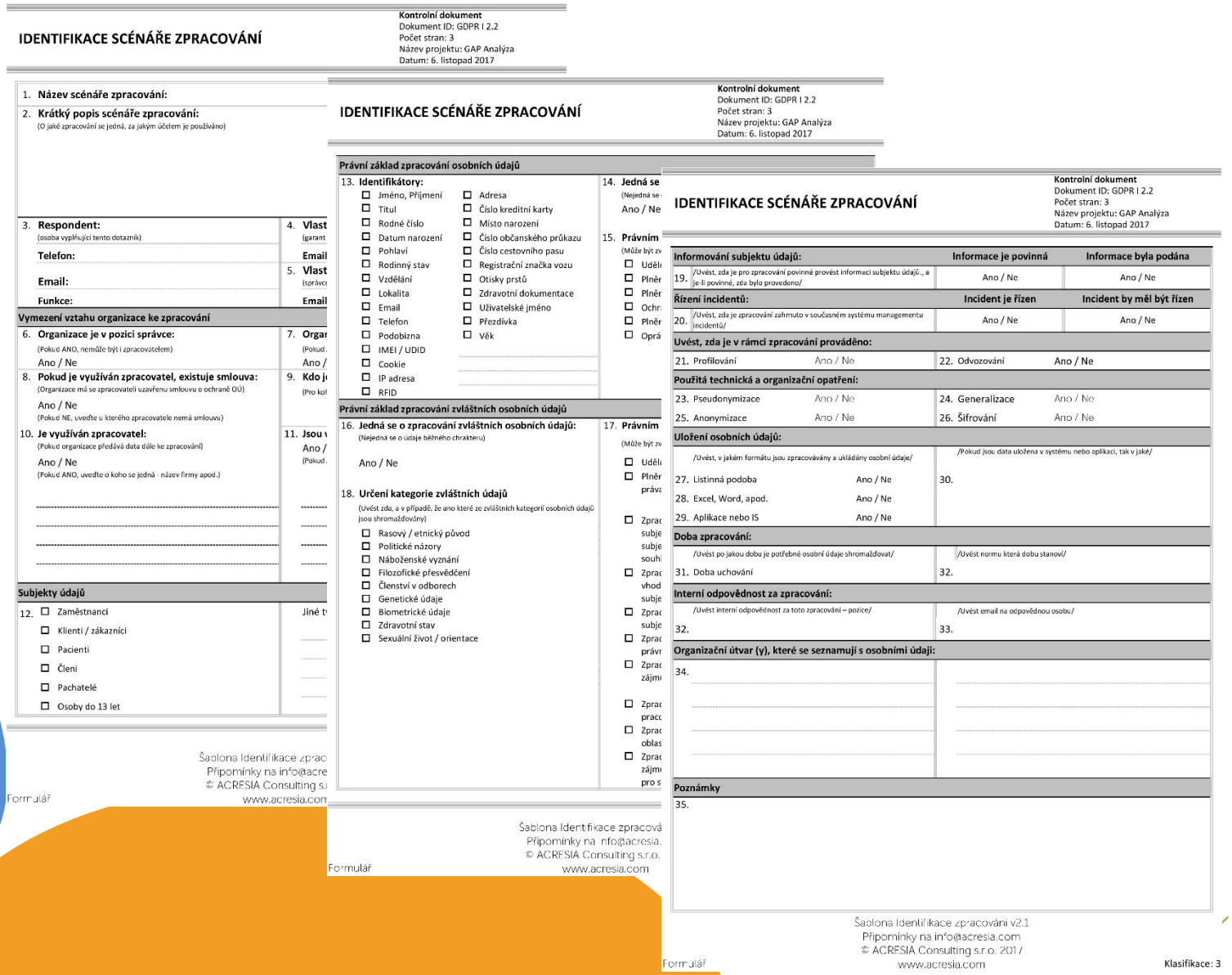
Cílem prověření stavu je:

- 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

ACRESIA CONSULTING

FORUM

Identifikace zpracování



IDENTIFIKACE SCÉNÁŘE ZPRACOVÁNÍ

Kontrolní dokument
Dokument ID: GDPR I 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
(správc
Email

Vymezení vztahu organizace ke zpracování

6. **Organizace je v pozici správce:**
(Pokud ANO, nemůže být i zpracovatelem)
Ano / Ne
7. Orga
(Pokud
Ano /
8. **Pokud je využíván zpracovatel, existuje smlouva:**
(Organizace má se zpracovateli uzavřenu smlouvu o ochraně OÚ)
Ano / Ne
(Pokud NE, uveďte u kterého zpracovatele nemá smlouvu)
9. Kdo j
(Pro kol
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 v
Ano /
(Pokud

Subjekty údajů

12. ☐ Zaměstnanci
☐ Klienti / zákazníci
☐ Pacienti
☐ Členi
☐ Pachatelé
☐ Osoby do 13 let
Jiné t

Šablona Identifikace zprac
Připomínky na info@acre
© ACRESIA Consulting s.
www.acresia.com
Formulář

IDENTIFIKACE SCÉNÁŘE ZPRACOVÁNÍ

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

Právní základ zpracování osobních údajů

13. **Identifikátory:**
- ☐ Jméno, Příjmení
- ☐ Titul
- ☐ Rodné číslo
- ☐ Datum narození
- ☐ Pohlaví
- ☐ Rodinný stav
- ☐ Vzdělání
- ☐ Lokalita
- ☐ Email
- ☐ Telefon
- ☐ Podobizna
- ☐ IMEI / UDID
- ☐ Cookie
- ☐ IP adresa
- ☐ RFID
- ☐ Adresa
- ☐ Číslo kreditní karty
- ☐ Místo narození
- ☐ Číslo občanského průkazu
- ☐ Číslo cestovního pasu
- ☐ Registrační značka vozu
- ☐ Otisky prstů
- ☐ Zdravotní dokumentace
- ☐ Uživatelské jméno
- ☐ Přezdívka
- ☐ Věk

14. Jedná se
(Nejedná se
Ano / Ne
15. Právním
(Může být zv
☐ Uděl
☐ Plněr
☐ Plněr
☐ Ochr
☐ Plněr
☐ Oprá

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

17. Právním
(Může být zv
☐ Uděl
☐ Plněr
práva
☐ Zprac
subje
subje
souhl
☐ Zprac
vhod
subje
☐ Zprac
subje
☐ Zprac
právn
☐ Zprac
zájmu
☐ Zprac
prac
☐ Zprac
oblas
☐ Zprac
zájmu
pro s

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

IDENTIFIKACE SCÉNÁŘE ZPRACOVÁNÍ

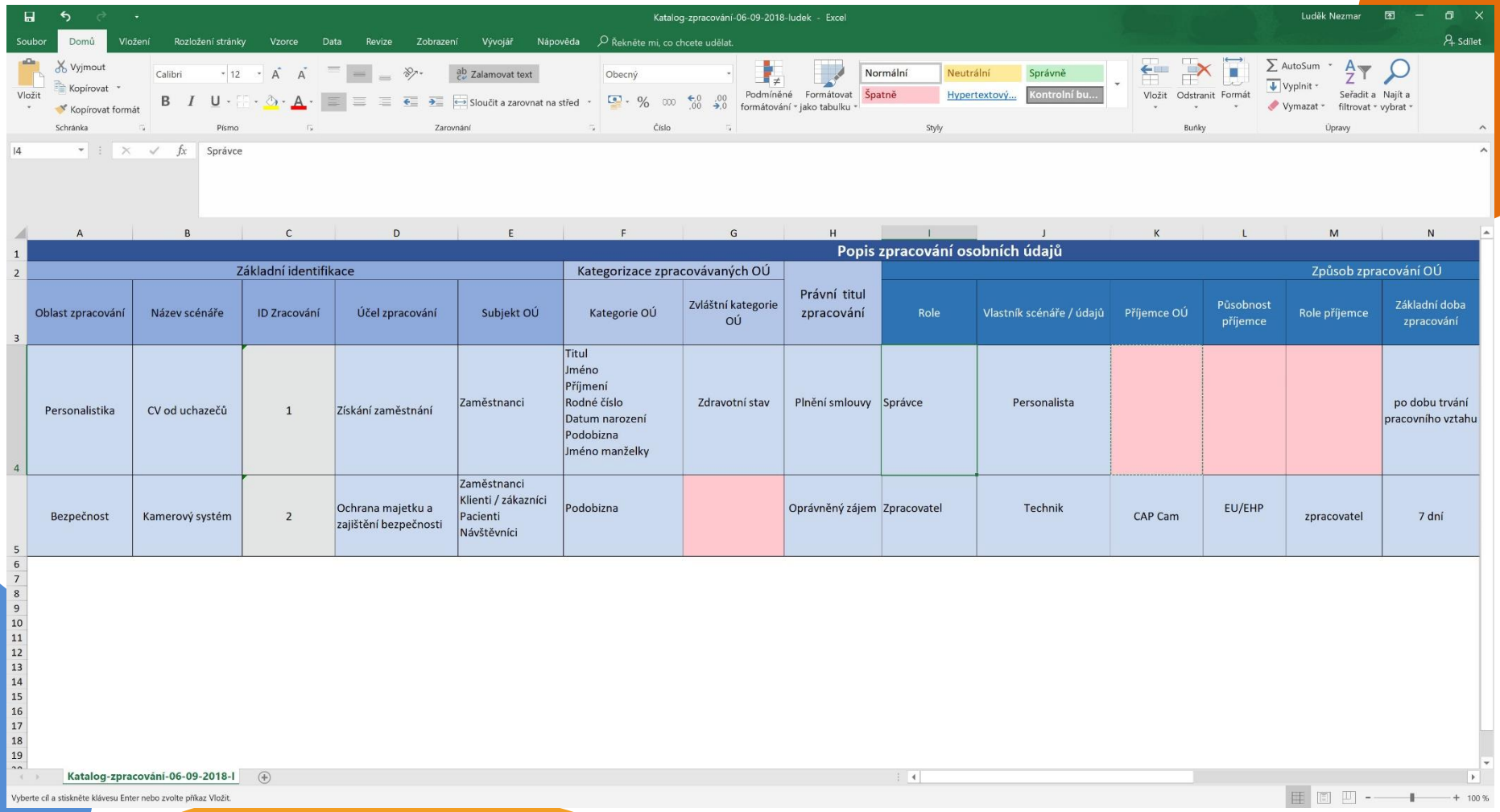
Kontrolní dokument
Dokument ID: GDPR I 2.2
Počet stran: 3
Název projektu: GAP Analýza
Datum: 6. listopad 2017

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 byla provedena/		Ano / Ne	Ano / Ne
Řízení incidentů:		**Incident je řízen**	**Incident by měl být řízen**
20. /Uvést, zda je zpracování zahrnuto v současném systému managementu incidentů/		Ano / Ne	Ano / Ne
Uvést, 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.		33.	
Organizační útvar (y), které se seznamují s osobními údaji:			
34.			
Poznámky			
35.			

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

Klasifikace: 3

Katalog zpracování



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

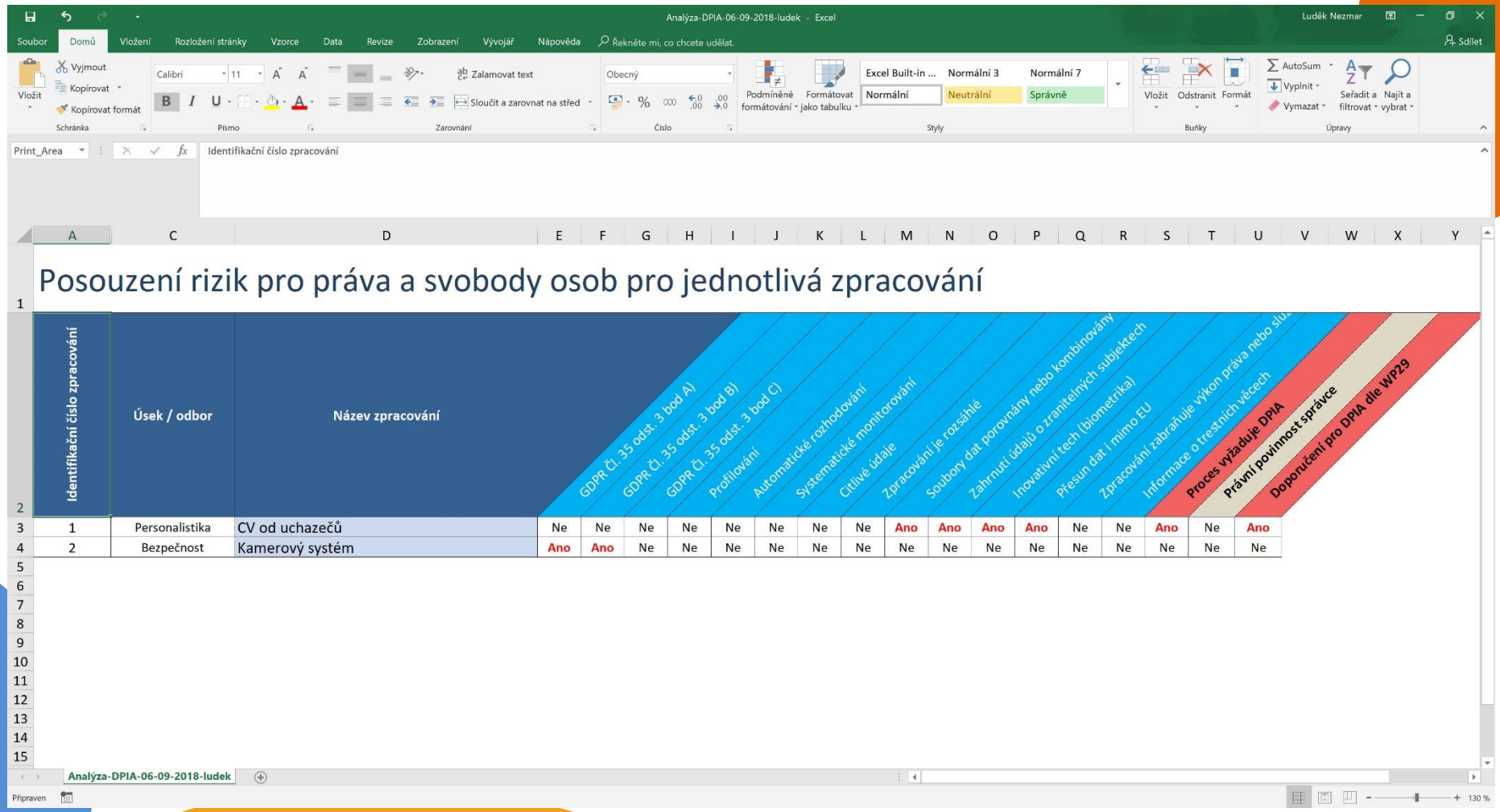
Správce

Popis zpracování osobních údajů													
Základní identifikace					Kategorizace zpracovávaných OÚ		Právní titul zpracování	Způsob zpracování OÚ					
Oblast zpracování	Název scénáře	ID Zracování	Účel zpracování	Subjekt OÚ	Kategorie OÚ	Zvláštní kategorie OÚ		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

ACRESIA CONSULTING

FORUM

Analýza DPIA



ACRESIA CONSULTING

FORUM

Analýza rizik zpracování osobních údajů

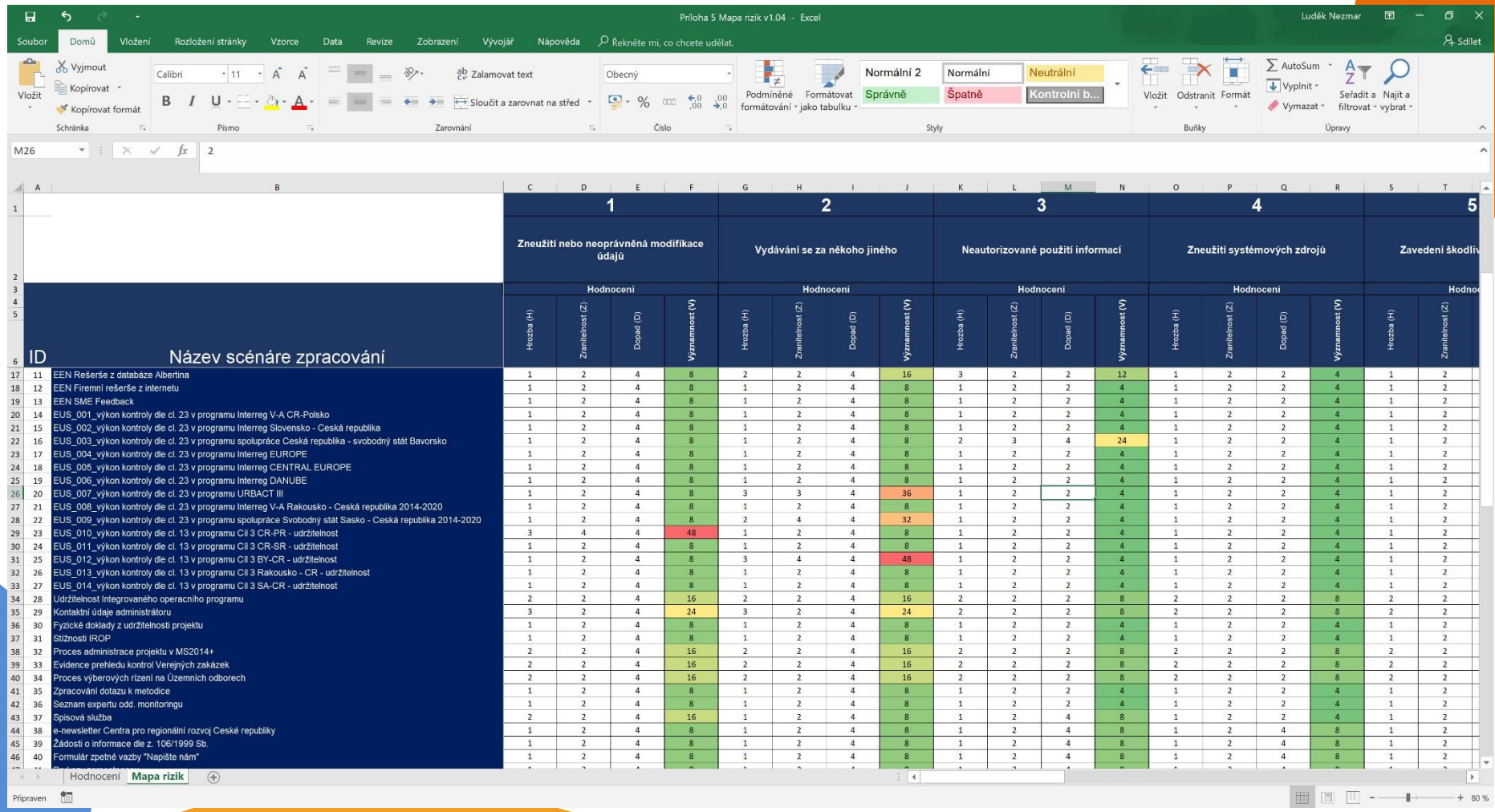
Posouzení rizik, či jak GDPR definuje „vyhodnocení hrozeb pro práva a svobody fyzických osob“ je možné provést v následujících krocích:

- 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

ACRESIA CONSULTING

FORUM

Analýza rizik – varianta 1



			1				2				3				4				5	
			Zneužití nebo neoprávněná modifikace údajů				Vydávání se za někoho jiného				Neautorizované použití informací				Zneužití systémových zdrojů				Zavedení škodliv	
			Hodnocení				Hodnocení				Hodnocení				Hodnocení				Hodno	
ID	Název scénáře zpracování		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 Rešerše z databáze Albertina		1	2	4	8	2	2	4	16	3	2	2	12	1	2	2	4	1	2
12	EEN Firemní rešerše 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_výkon kontroly dle 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_výkon kontroly dle cl. 23 v programu Interreg Slovensko - Ceská republika		1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
16	EUS_003_výkon kontroly dle cl. 23 v programu spolupráce Ceská 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_výkon kontroly dle 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_výkon kontroly dle 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_výkon kontroly dle 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_výkon kontroly dle 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_výkon kontroly dle cl. 23 v programu Interreg V-A Rakousko - Ceská republika 2014-2020		1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
22	EUS_009_výkon kontroly dle cl. 23 v programu spolupráce Svobodný stát Sasko - Ceská republika 2014-2020		1	2	4	8	2	4	4	32	1	2	2	4	1	2	2	4	1	2
23	EUS_010_výkon kontroly dle cl. 13 v programu Cil 3 CR-PR - udržitelnost		3	4	4	48	1	2	4	8	1	2	2	4	1	2	2	4	1	2
24	EUS_011_výkon kontroly dle cl. 13 v programu Cil 3 CR-SR - udržitelnost		1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
25	EUS_012_výkon kontroly dle cl. 13 v programu Cil 3 BY-CR - udržitelnost		1	2	4	8	3	4	4	48	1	2	2	4	1	2	2	4	1	2
26	EUS_013_výkon kontroly dle cl. 13 v programu Cil 3 Rakousko - CR - udržitelnost		1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
27	EUS_014_výkon kontroly dle cl. 13 v programu Cil 3 SA-CR - udržitelnost		1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
28	Udržitelnost Integrovaného operacního programu		2	2	4	16	2	2	4	16	2	2	2	8	2	2	2	8	2	2
29	Kontaktní údaje administrátoru		3	2	4	24	3	2	4	24	2	2	2	8	2	2	2	8	2	2
30	Fyzické doklady z udržitelnosti projektu		1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
31	Stížnosti IROP		1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
32	Proces administrace projektu v MS2014+		2	2	4	16	2	2	4	16	2	2	2	8	2	2	2	8	2	2
33	Evidence prehledu kontrol Verejných zakázek		2	2	4	16	2	2	4	16	2	2	2	8	2	2	2	8	2	2
34	Proces výberových rízení na Územních odborech		2	2	4	16	2	2	4	16	2	2	2	8	2	2	2	8	2	2
35	Zpracování dotazu k metodice		1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
36	Seznam expertu odd. monitoringu		1	2	4	8	1	2	4	8	1	2	2	4	1	2	2	4	1	2
37	Spisová služba		2	2	4	16	1	2	4	8	1	2	4	8	1	2	2	4	1	2
38	e-newsletter Centra pro regionální rozvoj Ceské republiky		1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8	1	2
39	Žádosti o informace dle z. 106/1999 Sb.		1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8	1	2
40	Formulár zpetné vazby "Napište nám"		1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8	1	2

ACRESIA CONSULTING

FORUM

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 oc údajů)
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 osob

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

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 generalizace OÚ**
(Systém využívá generalizace 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 šifrovaný kanál** (Systém využívá k přenosu dat šifrované spojení) Ano / Ne	21. **Aplikace využívá k přístupu systém rolí** (Systém využívá přístupy k datům dle pracovních pozic) Ano / Ne
22. **Aplikace vede auditní systém záznamů** (Systém loguje přístupy uživatelů a manipulaci s daty) Ano / Ne	23. **Aplikace využívá dvou faktorové ověření** (Systém používá k ochraně dat dvou faktorové zabezpečení) Ano / Ne
24. **Aplikace je sledována v SIEM/SOC** (Systém je napojen na doménu 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 redundanci nebo replikaci) Ano / Ne	27. **Aplikace je pravidelně zálohována** (Systém a jeho data jsou pravidelně zálohována) Ano / Ne
GDPR oddíl 2, článek 32, bod 1 c) - obnova dostupnosti a přístupu v případě 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 systému 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 zranitelnosti** (Je prováděno pravidelné testování zranitelností / 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)

Exitující 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 jasně definovány (skupina, holding vs. dceřiné společnosti,**
6. **Zaměstnanci jsou školeni v oblasti ochra**
jsou přijata opatření na zvyšování pově
Ano / Ne
8. **Výběr zpracovatelů a poskytovatelů slu**
na definovaných kritériích výběru a audit

Smlouvy se zpracovteli zahrnují

10. **Smlouvy zahrnují zajištění zničení dat po**
smlouvy nebo po skončení zpracování:
Ano / Ne / Pouze pro některé
12. **Smlouvy zahrnují pravidla pro subdodava**
zpracování:
Ano / Ne / Pouze pro některé
14. **Smlouvy zahrnují právo na audit zpracov**
údajů:
Ano / Ne / Pouze pro některé

IDENTIFIKACE OPATŘENÍ

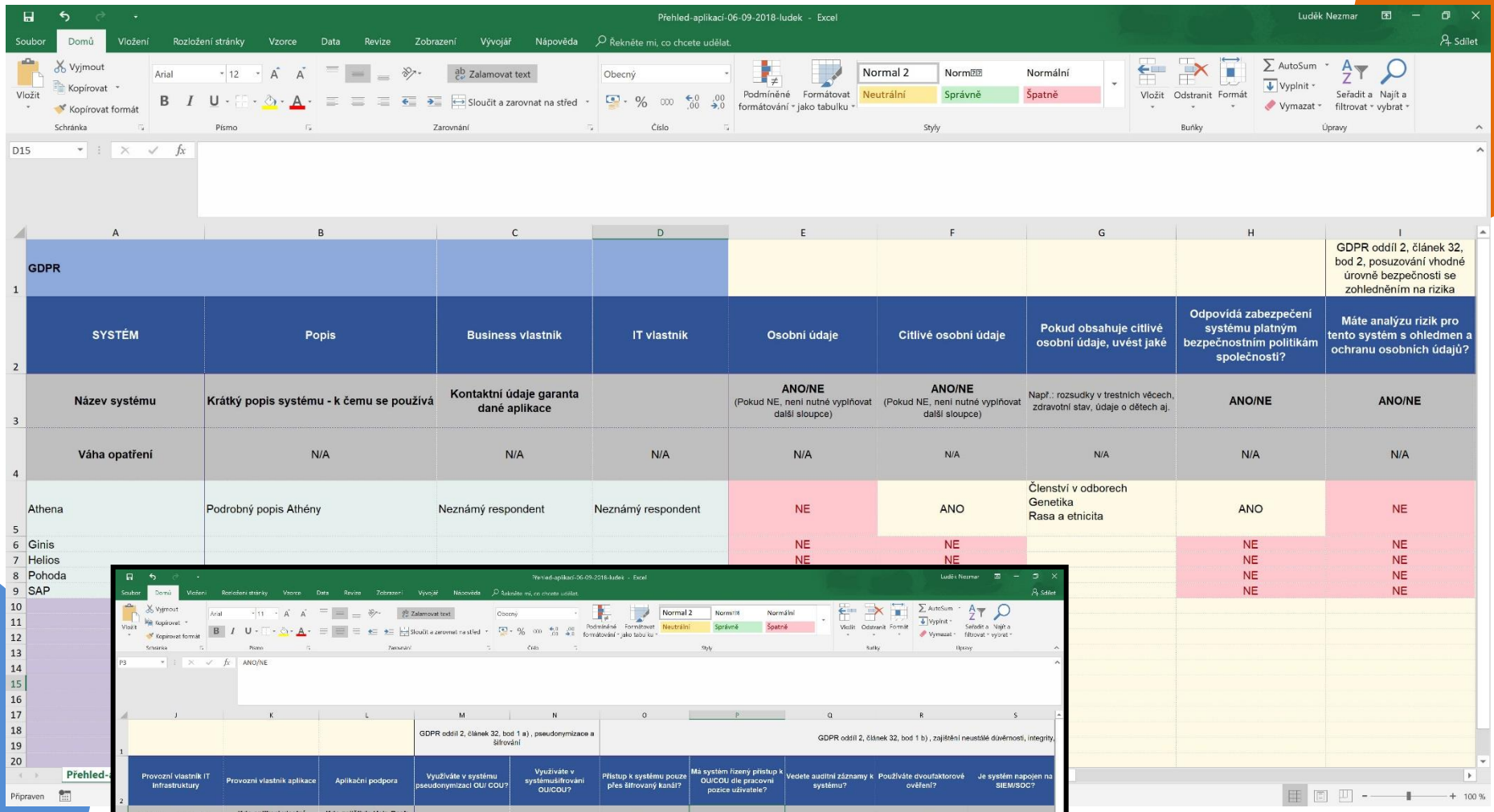
Kontrolní dokument
Dokument ID: GDPR I 3.1
Počet stran: 2
Název projektu: GAP Analýza
Datum: 2. listopad 2017

Bezpečnostní opatření	
16. **Je využíván princip "Potřeba vědět" pro určení rolí a autorizaci:** 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 zabezpečený pokročilými bezpečnostními opatřeními jako např. federated identity, certifikát, 2-faktorové ověřování:** Ano / Ne	23. **Přístup k zálohám a kopiím dat (zejména karty USB/HDD) 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, datová 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	

ACRESIA CONSULTING

FORUM

Analýza rizik – aplikace



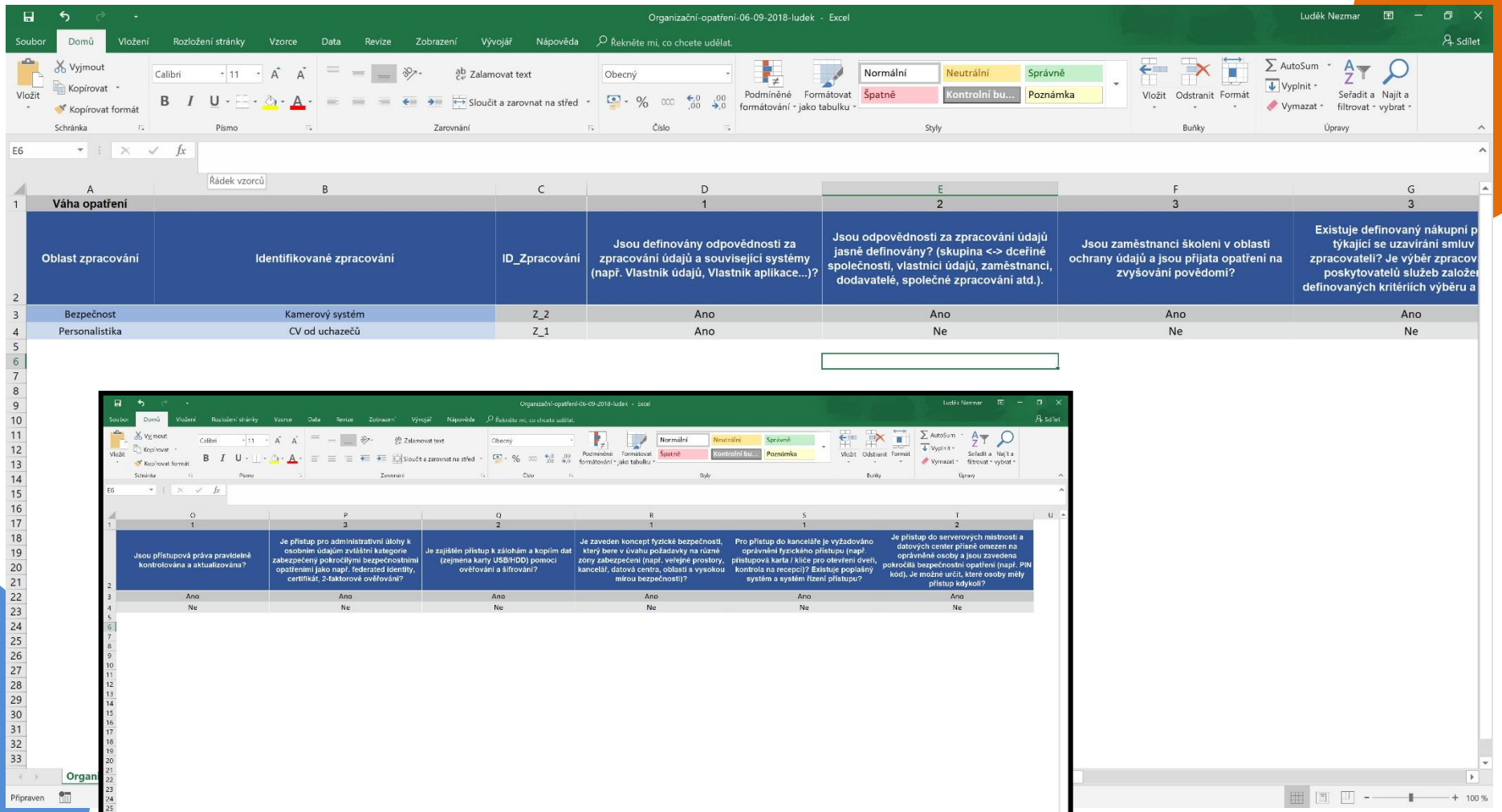
	A	B	C	D	E	F	G	H	I
1	GDPR								GDPR oddíl 2, článek 32, bod 2, posuzování vhodné úrovně bezpečnosti se zohledněním na rizika
2	SYSTÉM	Popis	Business vlastník	IT vlastník	Osobní údaje	Citlivé osobní údaje	Pokud obsahuje citlivé osobní údaje, uvést jaké	Odpovídá zabezpečení systému platným bezpečnostním politikám společnosti?	Máte analýzu rizik pro tento systém s ohledmen a 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
9	SAP							NE	NE

	J	K	L	M	N	O	P	Q	R	S
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	Provozní vlastník IT Infrastruktury	Provozní vlastník aplikace	Aplikační podpora	Využíváte v systému pseudonymizaci OU/ COU?	Využíváte v systému šifrování OU/COU?	Přístup k systému pouze přes šifrovaný kanál?	Má systém řízený přístup k OU/COU dle pracovní pozice uživatele?	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	NE	ANO	NE	NE
8				ANO	ANO	ANO	ANO	ANO	ANO	ANO
9				NE	NE	NE	NE	NE	NE	NE

ACRESIA CONSULTING

FORUM

Analýza rizik - opatření



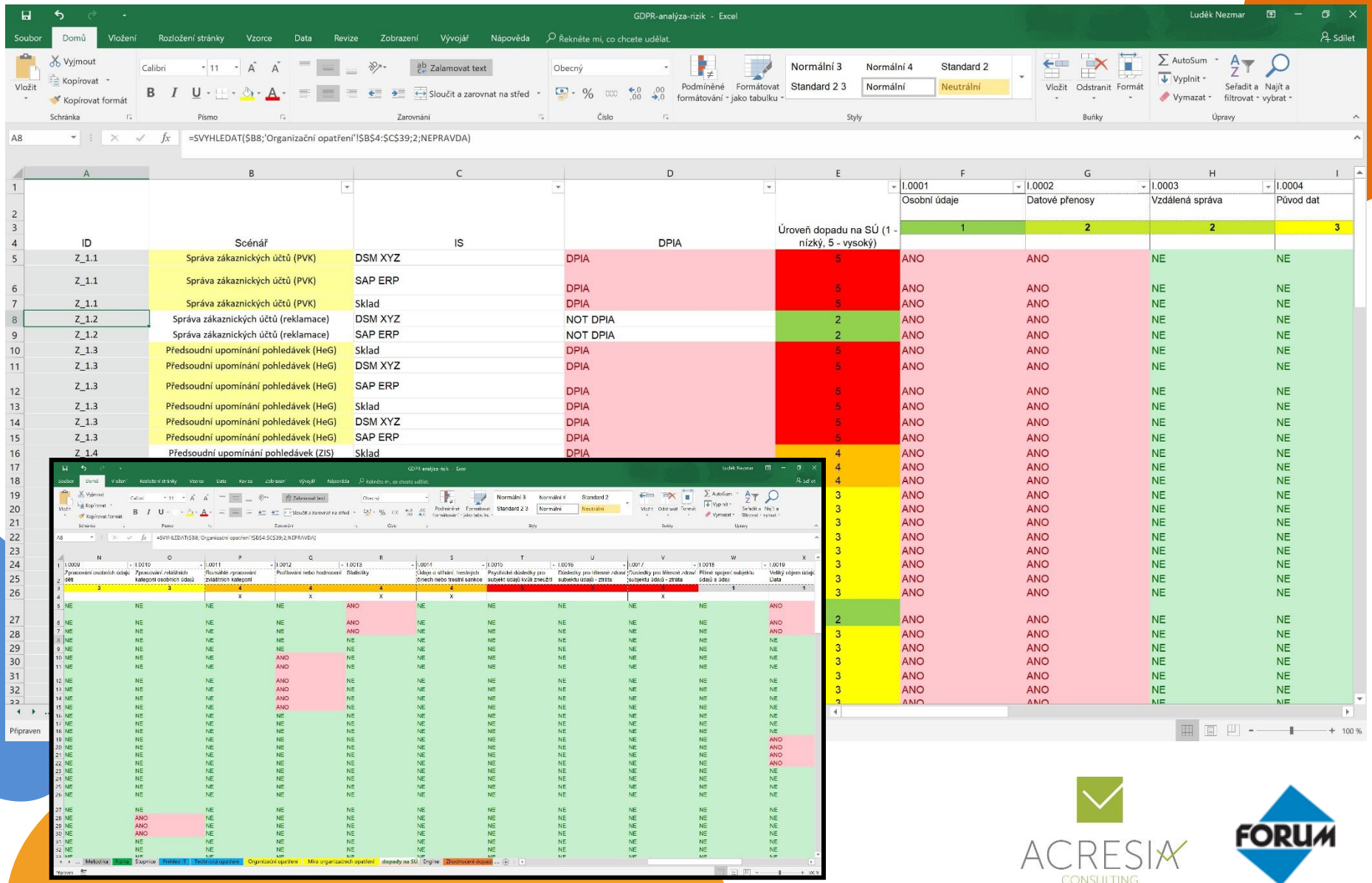
Váha opatření			1	2	3	3
Oblast zpracování	Identifikované zpracování	ID_Zpracování	Jsou definovány odpovědnosti za zpracování údajů a související systémy (např. Vlastník údajů, Vlastník aplikace...)?	Jsou odpovědnosti za zpracování údajů jasně definovány? (skupina <-> dceřiné společnosti, vlastníci údajů,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

	1	3	2	1	1	2
	Jsou přístupová práva pravidelně kontrolována a aktualizována?	Je přístup pro administrativní úlohy k osobním údajům zvláštní kategorie zabezpečený 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, datová 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 popisný 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 měly přístup kdykoli?
3	Ano	Ano	Ano	Ano	Ano	Ano
4	Ne	Ne	Ne	Ne	Ne	Ne

ACRESIA CONSULTING

FORUM

Analýza rizik – dopady na SÚ

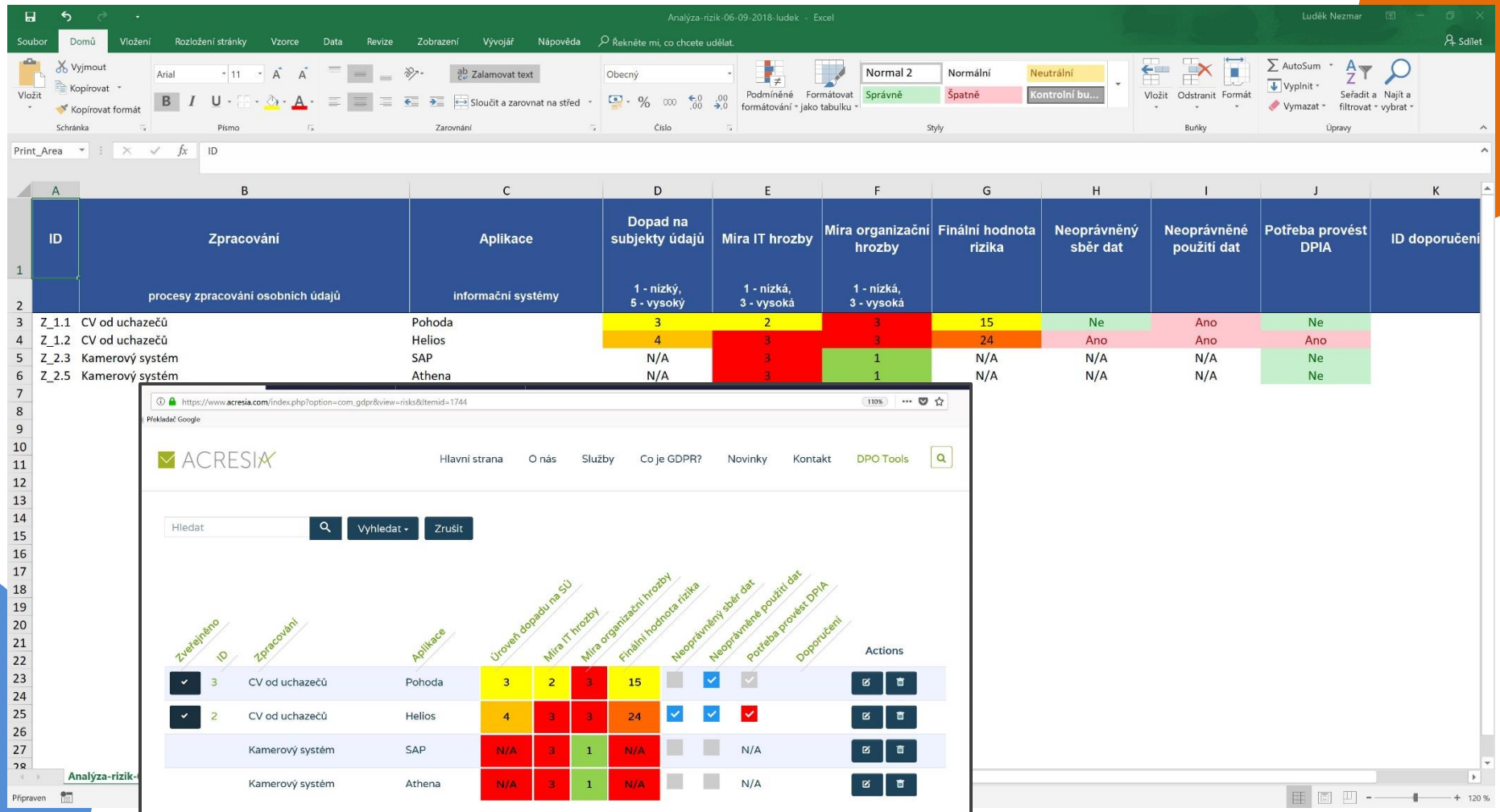


ID	Scénář	IS	DPIA	Úroveň dopadu na SÚ (1 - nízký, 5 - vysoký)	I.0001 Osobní údaje	I.0002 Datové přenosy	I.0003 Vzdálená správa	I.0004 Původ dat
					1	2	2	3
Z_1.1	Správa zákaznických účtů (PVK)	DSM XYZ	DPIA	5	ANO	ANO	NE	NE
Z_1.1	Správa zákaznických účtů (PVK)	SAP ERP	DPIA	5	ANO	ANO	NE	NE
Z_1.1	Správa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

ACRESIA CONSULTING

FORUM

Analýza rizik – výsledek



ID	Zpracování procesy zpracování osobních údajů	Aplikace informační systémy	Dopad na subjekty údajů 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	Potřeba provést DPIA	ID doporučení
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	

ACRESIA CONSULTING

FORUM

Posuzování vlivu na ochranu osobních údajů

Obsahem posouzení musí být:

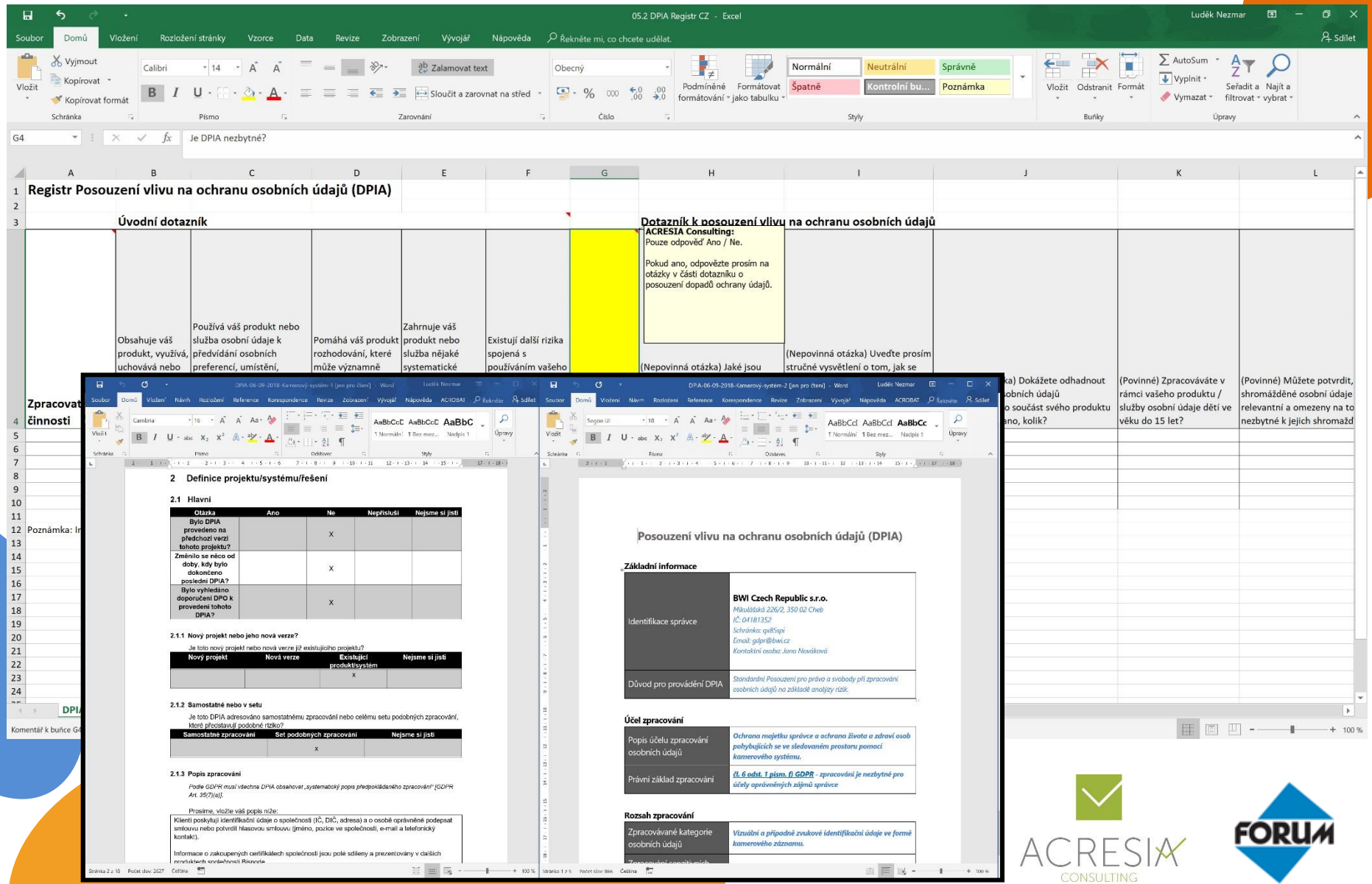
- Popis zamýšlených operací, účelů zpracování a oprávněných zájmů správce
- Zhodnocení nezbytnosti a proporcionality operací ve vztahu k účelům
- Zhodnocení rizika právům a svobodám jednotlivců
- Popis zamýšlených opatření ke zmírnění rizika, včetně bezpečnostních opatření a mechanismů

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

ACRESIA CONSULTING

FORUM

Registr DPIA



05.2 DPIA Registr CZ - Excel

Je DPIA nezbytné?

Registr Posouzení vlivu na ochranu osobních údajů (DPIA)

Úvodní dotazník

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.

Zpracovat činnosti

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 používáním vašeho

(Nepovinná otázka) Jaké jsou

(Nepovinná otázka) Uveďte prosím stručné vysvětlení o tom, jak se

a) Dokážete odhadnout sobních údajů o součást 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 omezeny na to nezbytné k jejich shromažd

Poznámka: Ir

DPIA-06-09-2018-Kamerový-systém-1 [jen pro čtení] - Word

2 Definice projektu/systému/řešení

2.1 Hlavní

Otázka	Ano	Ne	Nepřísluší	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 představují podobné riziko?

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, DIČ, adresa) a o osobě oprávněné podepsat smlouvu nebo potvrdit hlasovou smlouvu (jméno, pozice ve společnosti, e-mail a telefonický kontakt).

Informace o zakoupených certifikátech společnosti jsou poté sdíleny a prezentovány v dalších produktech společnosti Pinpoint.

DPIA-06-09-2018-Kamerový-systém-2 [jen pro čtení] - Word

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: qx85spi* *Email: gdpr@bwi.cz* *Kontaktní osoba: Jana 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*

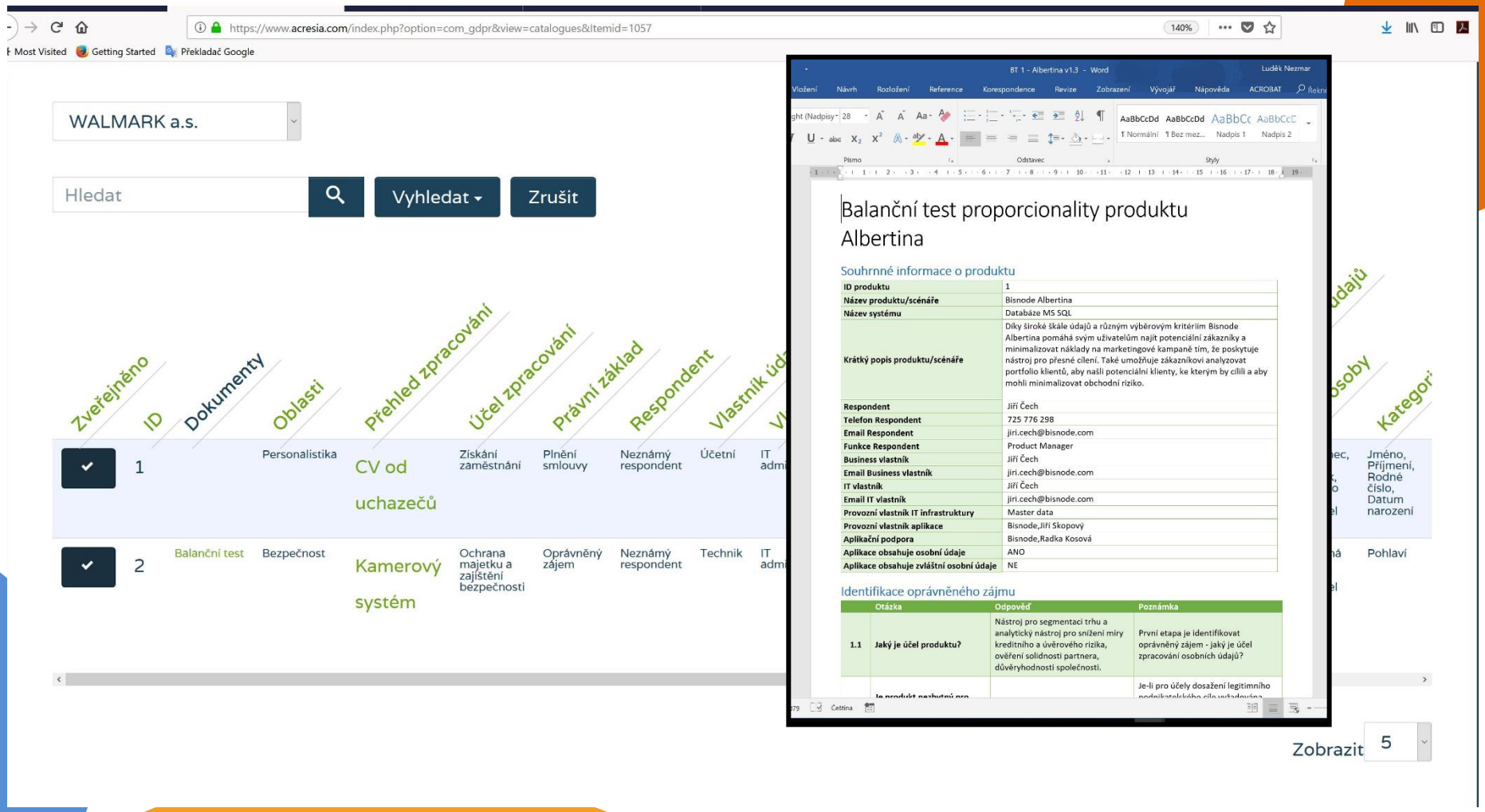
Rozsah zpracování

Zpracovávané kategorie osobních údajů	***Vizuální a případně zvukové identifikační údaje ve formě kamerového záznamu.***

ACRESIA CONSULTING

FORUM

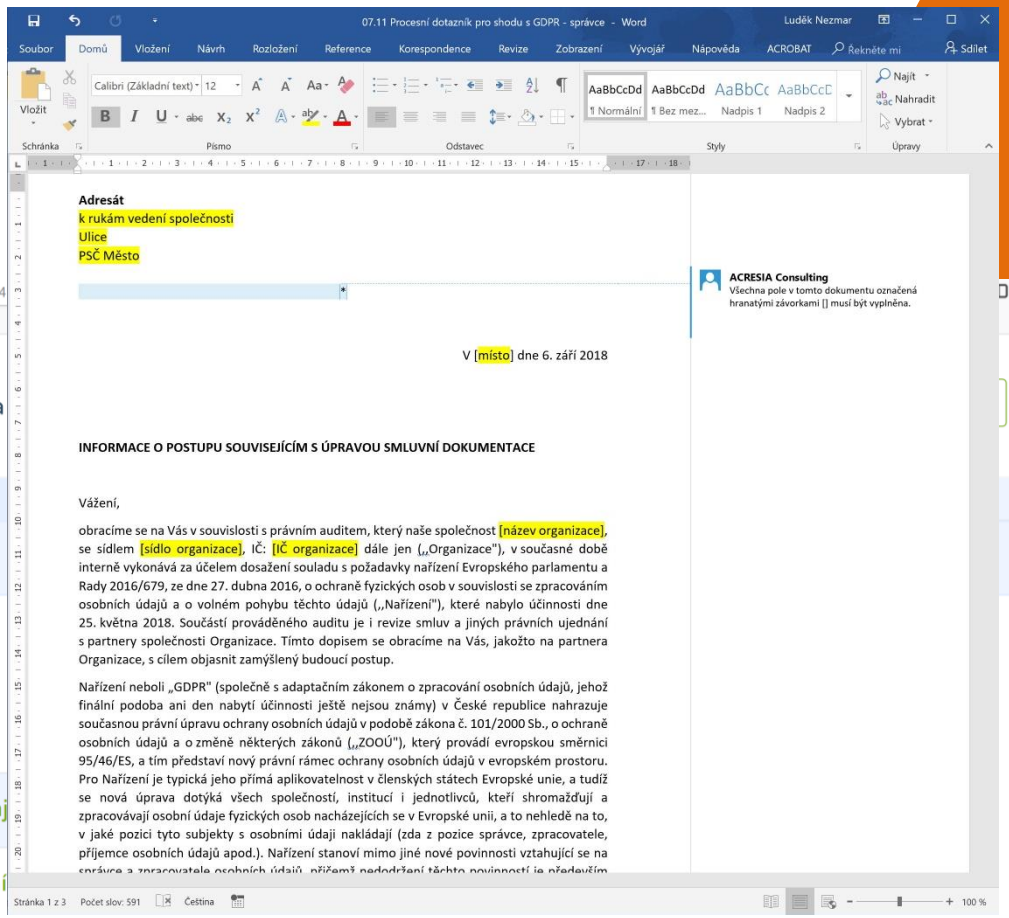
Balanční test proporcionality



ACRESIA CONSULTING

FORUM

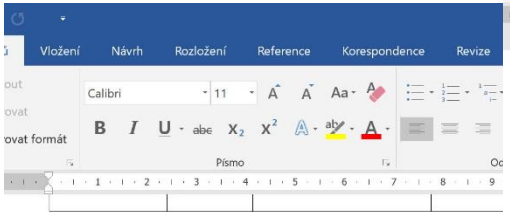
Zpracovatelé



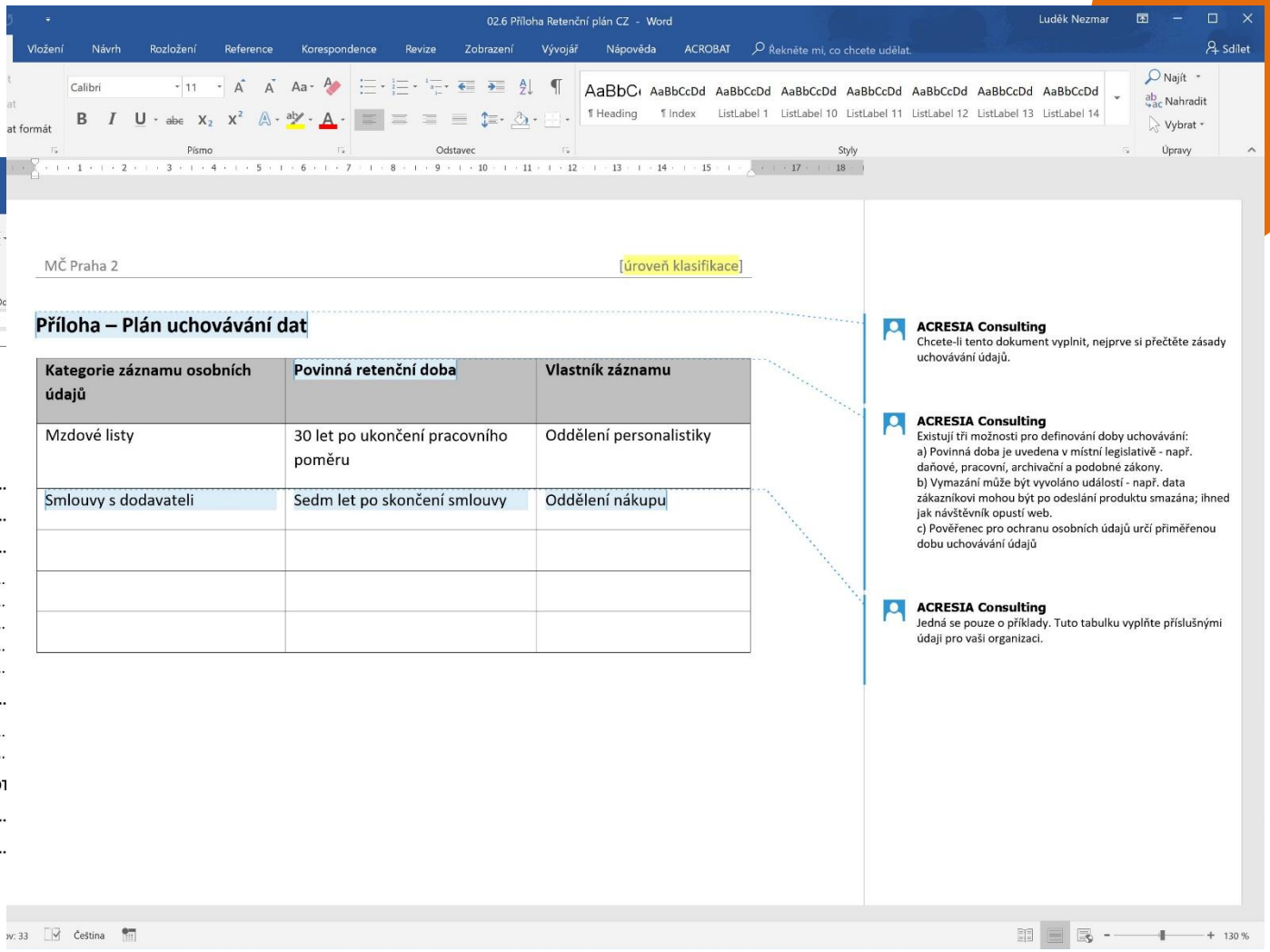
ACRESIA CONSULTING

FORUM

Retenční politika



Obsah



02.6 Příloha Retenční plán CZ - Word

MČ Praha 2 [úroveň klasifikace]

Příloha – Plán uchovávání 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 uchovávání údajů.

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

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

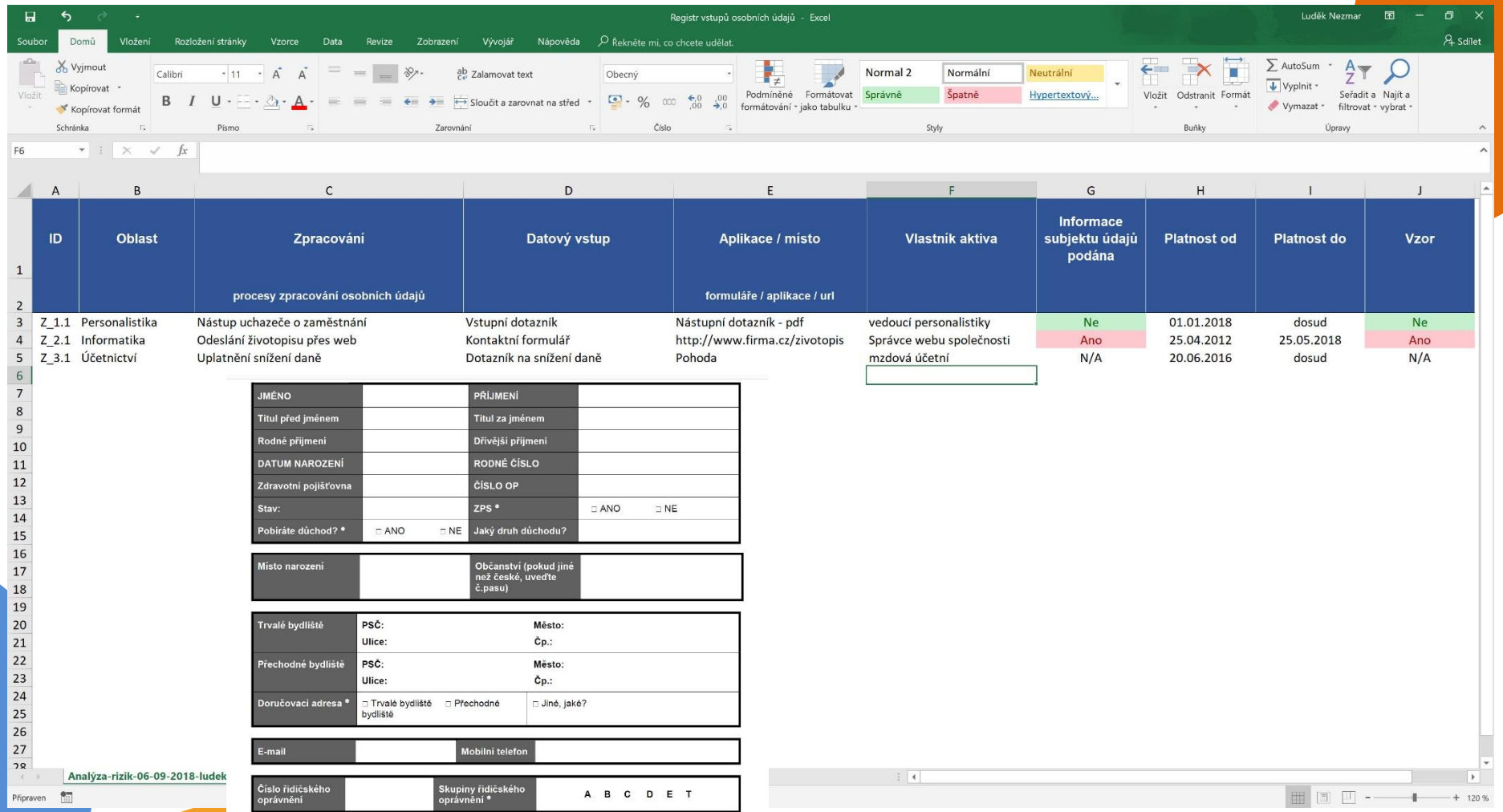
Pověřenec - DPO

- 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

ACRESIA CONSULTING

FORUM

Registr vstupů osobních údajů



Registr vstupů osobních údajů - Excel

ID	Oblast	Zpracování procesy zpracování osobních údajů	Datový vstup	Aplikace / místo formuláře / aplikace / url	Vlastník aktiva	Informace subjektu údajů podána	Platnost od	Platnost do	Vzor
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	Odeslání 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 *	☐ ANO ☐ NE
Pobíráte důchod? *	☐ ANO ☐ NE	Jaký druh důchodu?	

Místo narození		Občanství (pokud jiné než české, uveďte č.pasu)	

Trvalé bydliště	PSČ: Ulice:	Město: Čp.:	
Přechodné bydliště	PSČ: Ulice:	Město: Čp.:	
Doručovací adresa *	☐ Trvalé bydliště ☐ Přechodné bydliště	☐ Jiné, jaké?	

E-mail		Mobilní telefon	

Číslo řidičského oprávnění		Skupiny řidičského oprávnění *	A B C D E T

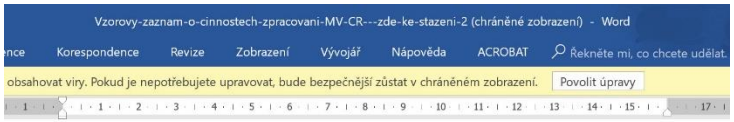
Rodinní příslušníci

Partner *	☐ Manžel/ka ☐ Druh/Družka	Jméno		Příjmení	
Rodné číslo					
Zaměstnán/a		Bydliště			
Jméno dítěte		Příjmení		Rodné číslo	

ACRESIA CONSULTING

FORUM

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 AGEND 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 pečetí.
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),

ACRESIA CONSULTING

FORUM

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

ACRESIA CONSULTING

FORUM

GDPR dokumentace

EU GDPR Složka dokumentace

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

Č.	Kód dokumentu	Název dokumentu	Odpovídající článe 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), 13 17, 30
10	2.6	Příloha - Plán uchovávání 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 (registr) 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)
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	Přeshraniční 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 správcům	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
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 zranitelností 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 subjekty 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 jednají v soudní moci; nebo b) se hlavní činnosti 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 zpracovávání rozsáhlých souborů zvláštních kategorií údajů podle článku 9 GDPR nebo osobní údaje týkající se odsouzení za trestný čin a trestných činů uvedených v článku 10 GDPR.

DPO a vedení organizace

DPO má výsadní postavení v rámci organizace:

- Interní vs. externí
- Samostatný vs. oddělení
- 100% pracovní náplň vs. dělená funkce
- Přístup k vedení organizace

Myšlenka ustanovení DPO pochází z úvahy nad rolí účetních a auditorů v organizacích, kteří také monitorují společnosti v zájmu dodržování předpisů.

ACRESIA CONSULTING

FORUM

Profesní kvality pověřence

„Pověřenec pro ochranu osobních údajů musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly stanovené v článku 39“.

Neexistuje povinnost certifikace pověřence

Nezbytná úroveň odborných znalostí by měla být určena zejména podle prováděných operací při zpracování osobních údajů a ochrany požadované pro osobní údaje zpracovávané správcem nebo zpracovatelem.

ACRESIA CONSULTING

FORUM

Profesní kvality pověřence

- profesní kvalifikaci nebo certifikaci vztahující se k ochraně osobních údajů a / nebo k informační bezpečnosti, zejména pak GDPR;
- odbornou znalost (zkušenost) nebo certifikaci vztahující se k oblasti, v níž operuje daná organizace;
- dostatečný stupeň znalosti práva, ideálně specializaci v ochraně osobních údajů, konkrétně zákona č. 101/2000 Sb. o ochraně osobních údajů a nařízení GDPR;
- zkušenosti s implementací ochrany dat, ISMS;
- zkušenosti se systémy a procesy spojenými se zabezpečením osobních údajů;
- zkušenost s problematikou personalistiky v rámci zpracování údajů;
- znalosti spojené s analýzou rizik;
- znalost práce marketingu, respektive způsobu zpracování osobních dat klientů;

ACRESIA CONSULTING

FORUM

Organizace by měla zajistit

- pravidelná účast na poradách vedení;
- přítomnost momentem, kdy jsou přijímána rozhodnutí mající důsledky na ochranu osobních údajů;
- relevantní informace musí být předány pověřenci včas, aby mu následně umožnily poskytnout odpovídající doporučení a rady;
- stanovisku pověřence musí být vždy věnována náležitá váha a pozornost;
- zdokumentovat důvody, proč nebylo uplatněno stanovisko nabízené pověřencem;
- pověřenec musí být okamžitě konzultován, pokud dojde k porušení dat nebo jinému incidentu ;

ACRESIA CONSULTING

FORUM

Nezbytné zdroje

- aktivní podpora funkce pověřence ze strany vrcholového vedení;
- pověřenec by měl mít dostatek času a prostoru k plnění svých povinností (stanovení procentního podílu);
- Přiměřená podpora finančními zdroji, infrastrukturou (prostory, zařízení, vybavení) a personálem;
- oficiální sdělení napříč organizací o jmenování;
- zajistit potřebný přístup k dalšímu servisu – IT, právní služby;
- zabezpečit průběžné školení;
- zřízení podpůrného týmu, pokud je třeba.

Nezávislý způsob

„nedostával žádné pokyny týkající se výkonu těchto úkolů. V souvislosti s plněním svých úkolů není správcem nebo zpracovatelem propuštěn ani sankcionován. Pověřenec pro ochranu osobních údajů je přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele“ čl. 38/3

- nesmí být instruován jak dosáhnout výsledku nebo jak řešit danou záležitost;
- nesmí být nucen vyjádřit svůj postoj k názoru na nějaké ustanovení zákona (výklad);
- samostatnost neznamená možnost rozhodovat mimo své kompetence;
- Odpovědnost zůstává správci a zpracovateli;

ACRESIA CONSULTING

FORUM

Odvolání nebo udělení trestu pověřenci

„v souvislosti s plněním svých úkolů není správcem nebo zpracovatelem propuštěn ani sankcionován“ čl. 38/3

- autonomie jak pověřenců, tak celých útvarů;
- sankce mohou být:
  - přímé;
  - nepřímé;
- stačí pouhá hrozba;
- jiné důvody jsou akceptovatelné.

Konflikt zájmů

- identifikovat pozice, které by byly neslučitelné s funkcí pověřence;
- vypracovat pro tento účel vnitřní pravidla, aby se předešlo střetu zájmů;
- zahrnout obecnější vysvětlení o konfliktech zájmů;
- veřejně prohlásit, že pověřenec pro ochranu osobních údajů nemá konflikt zájmů;
- zahrnout ochranná opatření do vnitřních předpisů organizace;
- oznámení o volném pracovním místě pověřence nebo smlouvy o poskytování služeb by mělo být dostatečně přesné a podrobné

ACRESIA CONSULTING

FORUM

Pověřenec – hlavní úkoly

- Pomoc při provádění DPIA
- Komunikace se subjekty osobních údajů
- Komunikace s Úřadem pro ochranu osobních údajů
- Sleduje soulad s legislativou týkající se ochrany osobních údajů a nařízením GDPR.
- Podává zprávy přímo vedení organizace
- Prosazuje přístup založený na riziku
- Dokumentuje a dále udržuje přehledy operací zpracování na základě informací od různých oddělení své organizace, zodpovědných za zpracování osobních údajů, a to včetně vedení registru (evidence).

ACRESIA CONSULTING

FORUM

Komunikace pověřence s ÚOOÚ

- Spolupracovat s dozorovým úřadem (ÚOOÚ) a být styčným bodem pro tento úřad
- Zajistit soulad společnosti s cíli GDPR a dalšími příslušnými právními předpisy
- Nastavení obhájitelných lhůt pro uchovávání osobních údajů
- Povolování nebo schvalování konkrétních pracovních postupů, které umožňují přístup k údajům
- Návrh způsobu anonymizace uchovaných dat
- Postup při pseudonymizaci dat
- Následné sledování všech těchto procesů

ACRESIA CONSULTING

FORUM

Neslučitelnost pozic s DPO

- neslučitelné pozice s DPO:
  - vedoucí oddělení HR;
  - vedoucí oddělení marketingu;
  - zaměstnanci IT oddělení;
  - ředitel;
  - finanční ředitel;
  - primář nebo šéf oddělení lékařské péče;
- nesmí existovat konflikt zájmů;
- externí právník - nelze

ACRESIA CONSULTING

FORUM

Vedení záznamů

- DPO není odpovědný za vedení záznamů
- Německo a Francie naopak
- správce nebo zpracovatel může tuto povinnost přiřadit DPO
- nástroj k plnění informační povinnosti a poradenství
- sledování souladu s GDPR

Na co dále nezapomenout

Identifikace zpracování	• Určení účelů a titulů zpracování • Určení podmínek zpracování
Pověřenec	• Vymezit činnosti, nasmlouvat jeho činnost • Vhodné hned po srovnávací analýze
Úprava klientských smluv a způsobu informování	• Úprava klientských smluv, zapracování povinných informací a úprava případného souhlasu
Zpracovatelské smlouvy	• Vymezení nových povinností Správce – Zpracovatel a úprava smluv
Posouzení vlivu a systém hlášení	• Příprava procesu (včetně zdokumentování) pro zpracování posouzení a hlášení
Vedení záznamů o zpracování	• Zdokumentování přijatých technických a organizačních opatření včetně testů a hodnocení

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

ACRESIA CONSULTING

FORUM

Děkuji za pozornost

www.forum-media.cz
www.acresia.com