ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

# GDPR

## Požadavky na dokumentaci

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)**

Zpracování osobních údajů se nemusí registrovat

ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

# 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

TECHNOLOGICKÉ CENTRUM AV ČR

# 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

TECHNOLOGICKÉ CENTRUM AV ČR

# Srovnávací analýza stavu

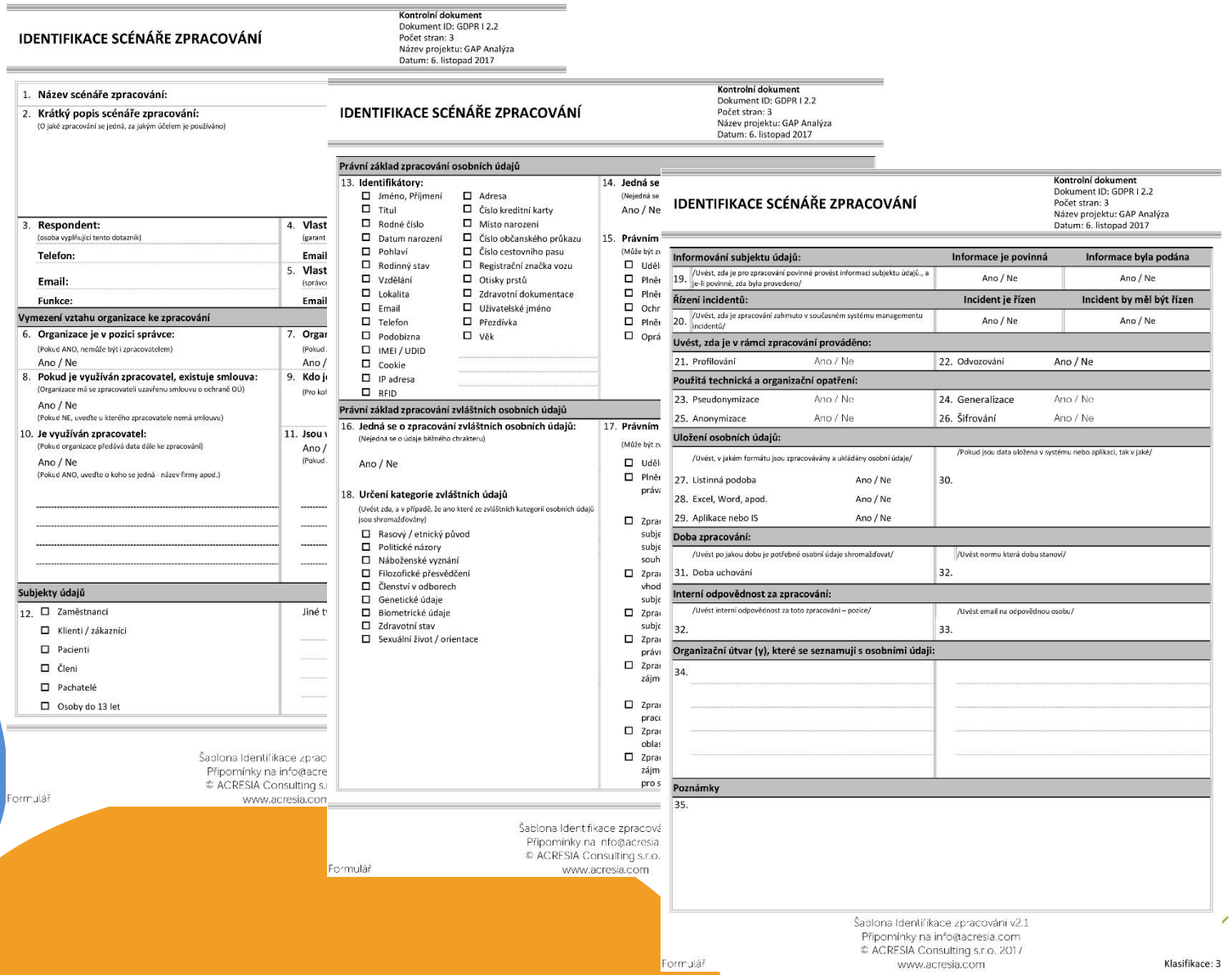
Cílem prověření stavu je:

- 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

TECHNOLOGICKÉ CENTRUM AV ČR

# 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 z
☐ Udě
☐ Plně
☐ Plně
☐ Ochr
☐ Plně
☐ Opra

**Právní základ zpracování zvláštních osobních údajů**

16. **Jedná se o zpracování zvláštních osobních údajů:**
(Nejedná se o údaje běžného charakteru)
Ano / Ne
17. Právním
(Může být z
☐ Udě
☐ Plně
práv

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

☐ Zprac
subje
subje
souh
☐ Zprac
vhod
subje
☐ Zprac
subje
☐ Zprac
právi
☐ Zprac
zájm
☐ Zprac
prac
☐ Zprac
oblas
☐ Zprac
zájm
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

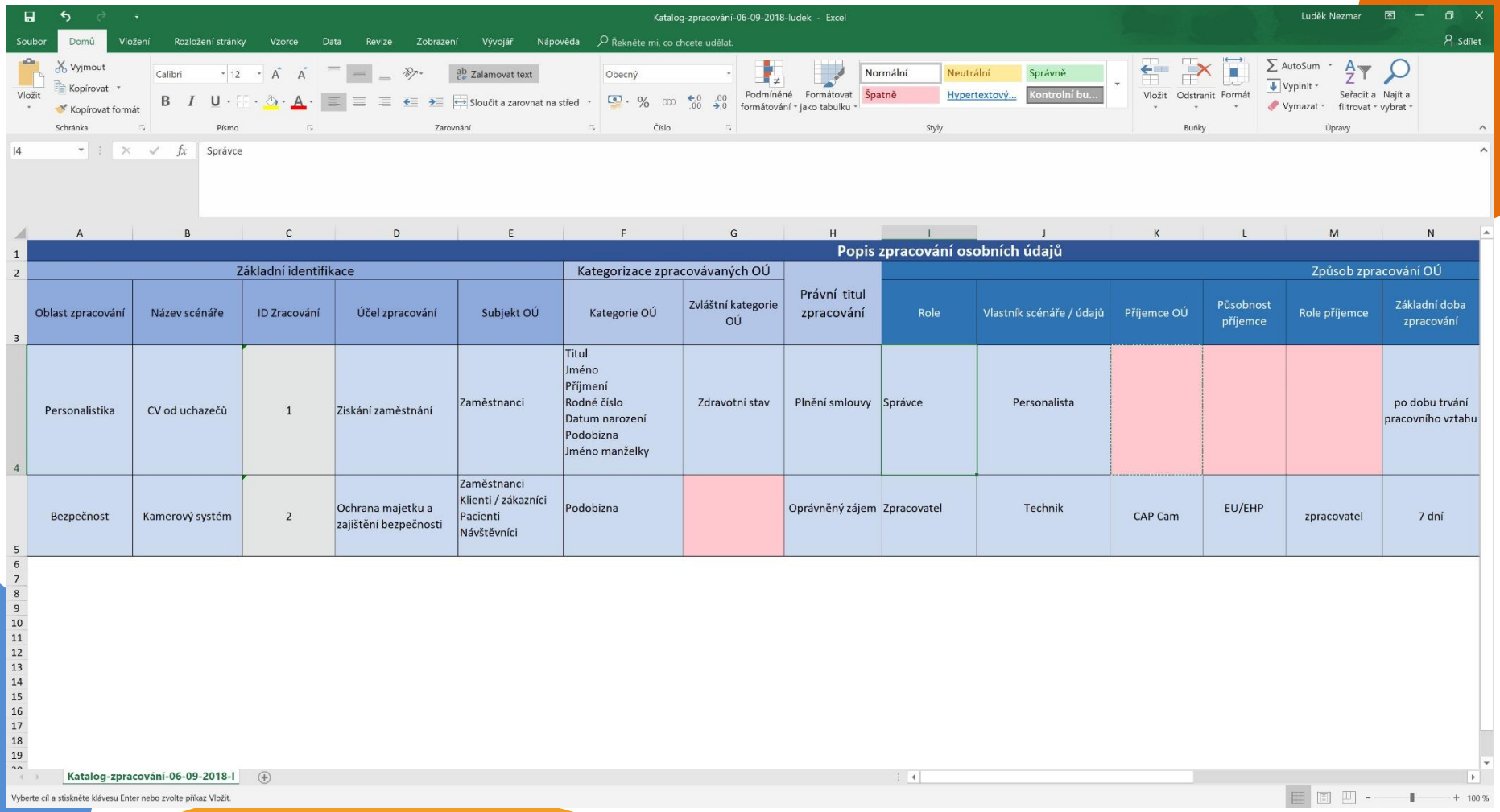
| Informování subjektu údajů: | | Informace je povinná | Informace byla podána |
|---|---|---|---|
| 19. /Uvést, zda je pro zpracování povinné provést informaci subjektu údajů., a je-li povinné, zda bylo provedeno/ | | Ano / Ne | Ano / Ne |
| **Řízení incidentů:** | | **Incident je řízen** | **Incident 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

TECHNOLOGICKÉ CENTRUM AV ČR

# Katalog zpracování



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

Luděk Nezmar

Soubor | Domů | Vložení | Rozložení stránky | Vzorce | Data | Revize | Zobrazení | Vývojář | Nápověda | Řekněte mi, co chcete udělat. | Sdílet

Vložit | Vyjmout | Kopírovat | Kopírovat formát | Schránka

Calibri | 12 | Písmo

Zalamovat text | Sloučit a zarovnat na střed | Zarovnání

Obecný | Číslo

Podmíněné formátování | Formátovat jako tabulku | Normální | Neutrální | Správně | Špatně | Hypertextový... | Kontrolní bu... | Styly

Vložit | Odstranit | Formát | Buňky

AutoSum | Vyplnit | Vymazat | Seřadit a filtrovat | Najít a vybrat | Úpravy

I4 | Správce

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Popis zpracování osobních údajů | | | | | | | | | | | | | |
| 2 | Základní identifikace | | | | | Kategorizace zpracovávaných OÚ | | Právní titul zpracování | Způsob zpracování OÚ | | | | | |
| 3 | 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 |
| 4 | Personalistika | CV od uchazečů | 1 | Získání zaměstnání | Zaměstnanci | Titul<br>Jméno<br>Příjmení<br>Rodné číslo<br>Datum narození<br>Podobizna<br>Jméno manželky | Zdravotní stav | Plnění smlouvy | Správce | Personalista | | | | po dobu trvání pracovního vztahu |
| 5 | Bezpečnost | Kamerový systém | 2 | Ochrana majetku a zajištění bezpečnosti | Zaměstnanci<br>Klienti / zákazníci<br>Pacienti<br>Návštěvníci | Podobizna | | Oprávněný zájem | Zpracovatel | Technik | CAP Cam | EU/EHP | zpracovatel | 7 dní |

Katalog-zpracování-06-09-2018-l

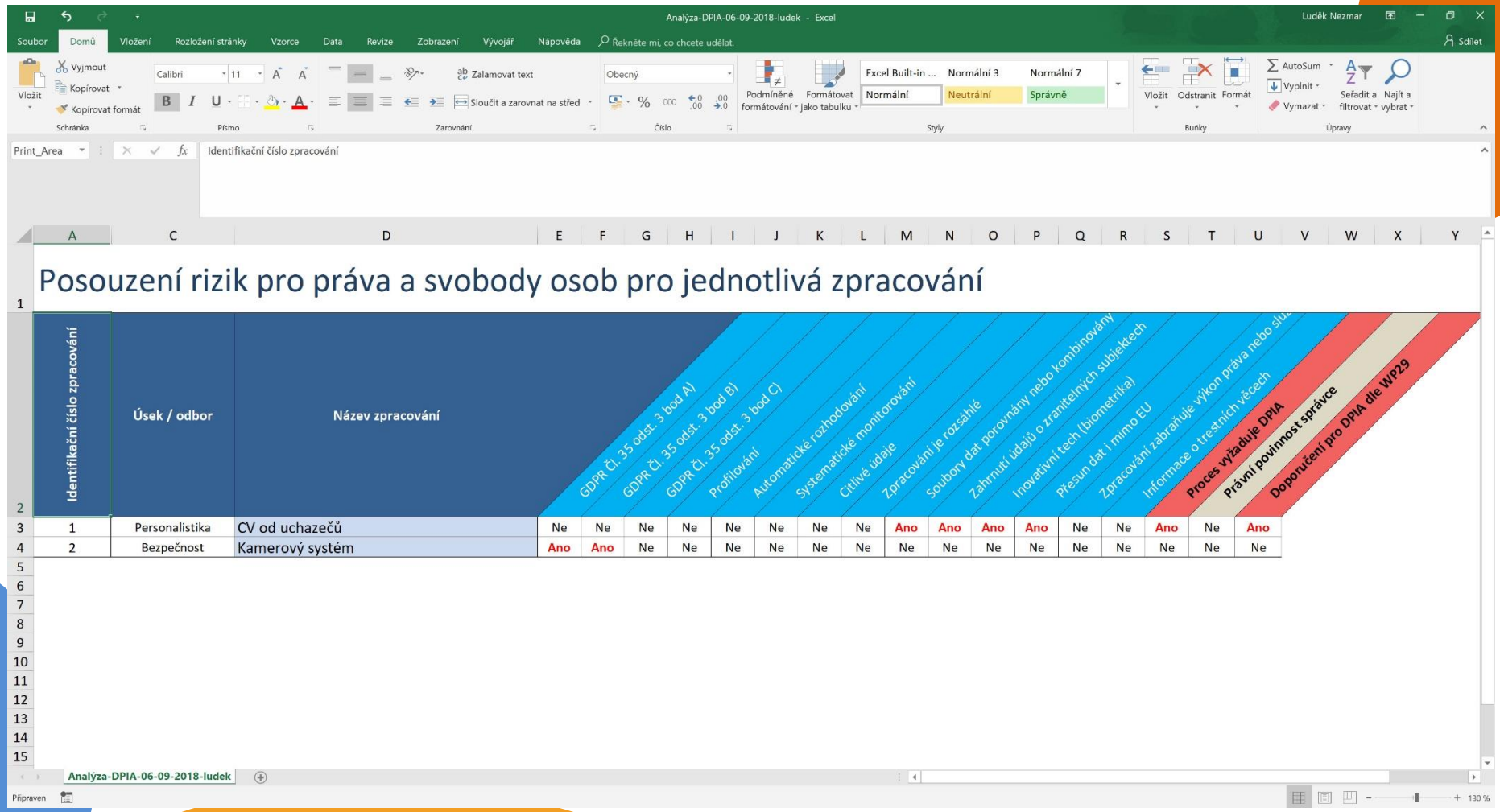
Vyberte cíl a stiskněte klávesu Enter nebo zvolte příkaz Vložit.

100 %

ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

# Analýza DPIA




ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

# Analýza rizik zpracování osobních údajů

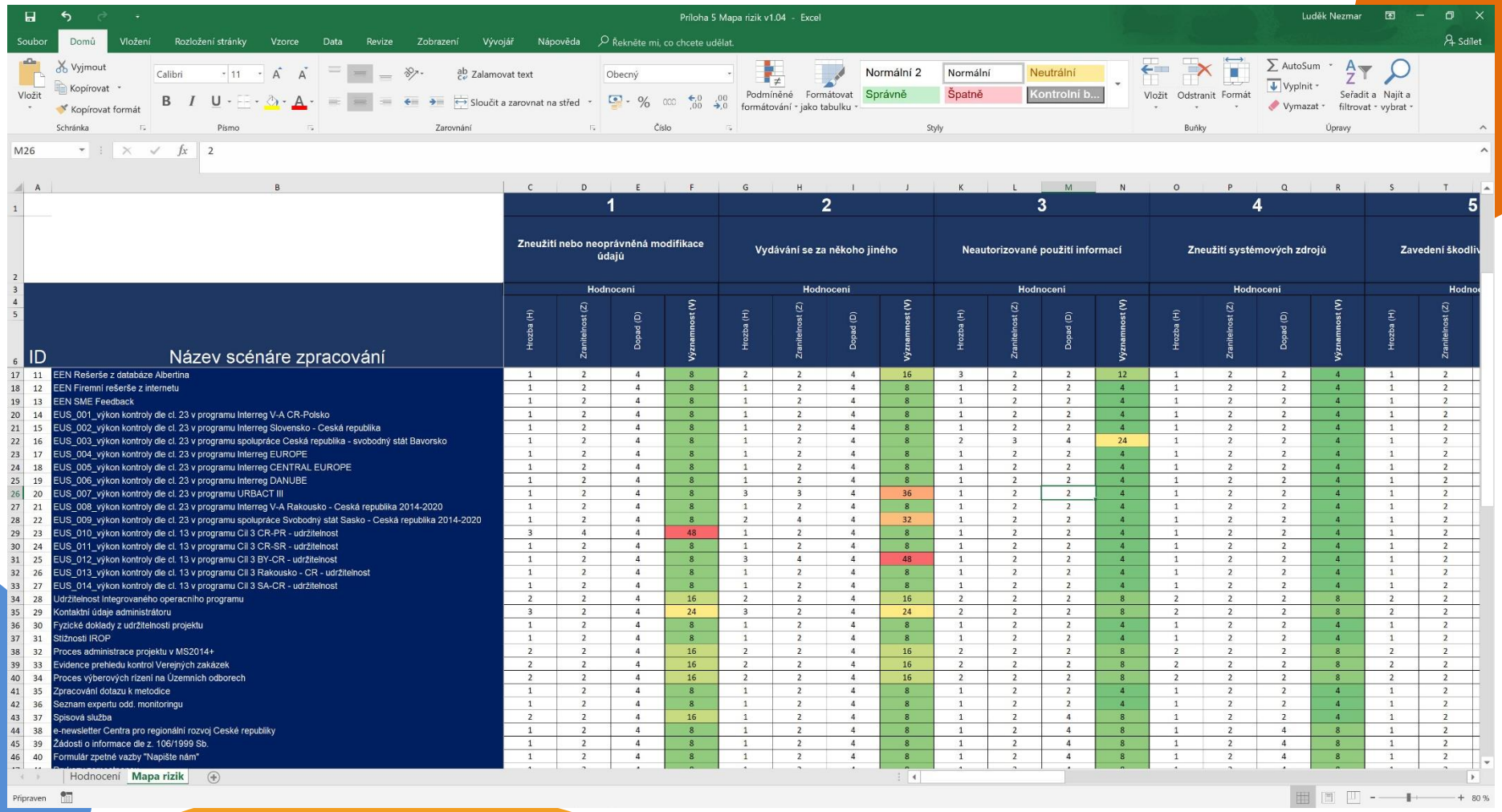
Posouzení rizik, či jak GDPR definuje „vyhodnocení hrozeb pro práva a svobody fyzických osob“ je možné provést v následujících krocích:

- 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

TECHNOLOGICKÉ CENTRUM AV ČR

# Analýza rizik – varianta 1



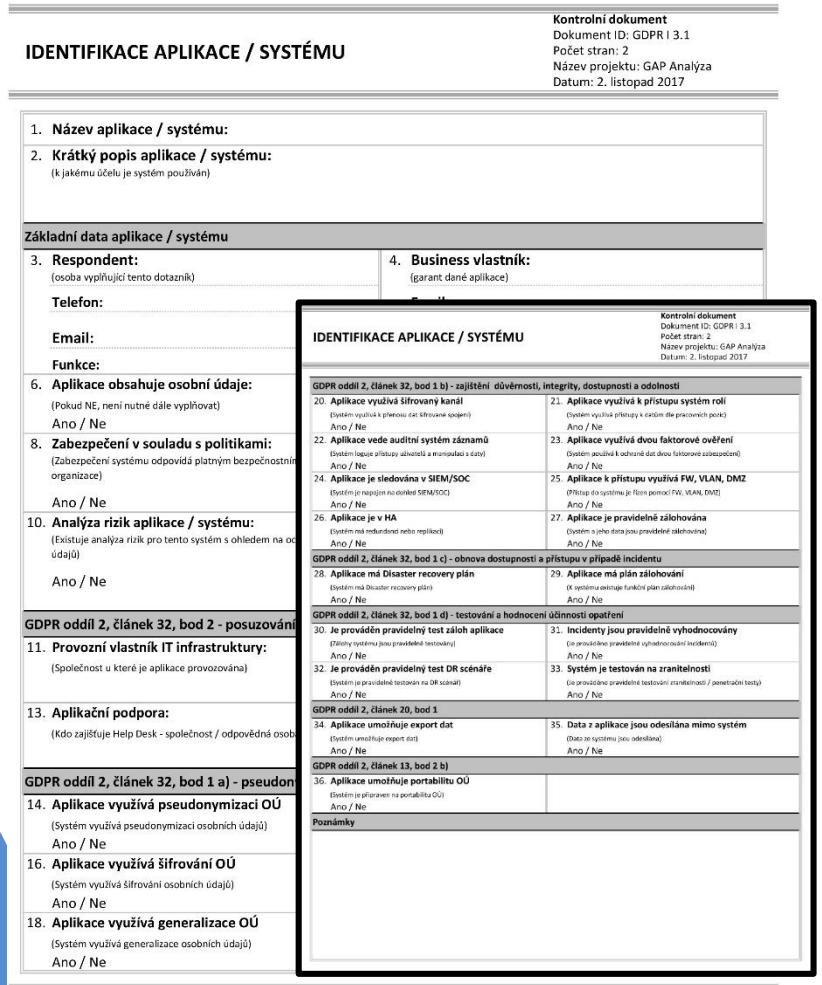
Příloha 5 Mapa rizik v1.04 - Excel

| ID | Název scénáře zpracování | 1 Zneužití nebo neoprávněná modifikace údajů | | | | 2 Vydávání se za někoho jiného | | | | 3 Neautorizované použití informací | | | | 4 Zneužití systémových zdrojů | | | | 5 Zavedení škodliv | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Hodnocení | | | | Hodnocení | | | | Hodnocení | | | | Hodnocení | | | | Hodnoc | |
| | | 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

TECHNOLOGICKÉ CENTRUM AV ČR

# 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 doručení 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 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**

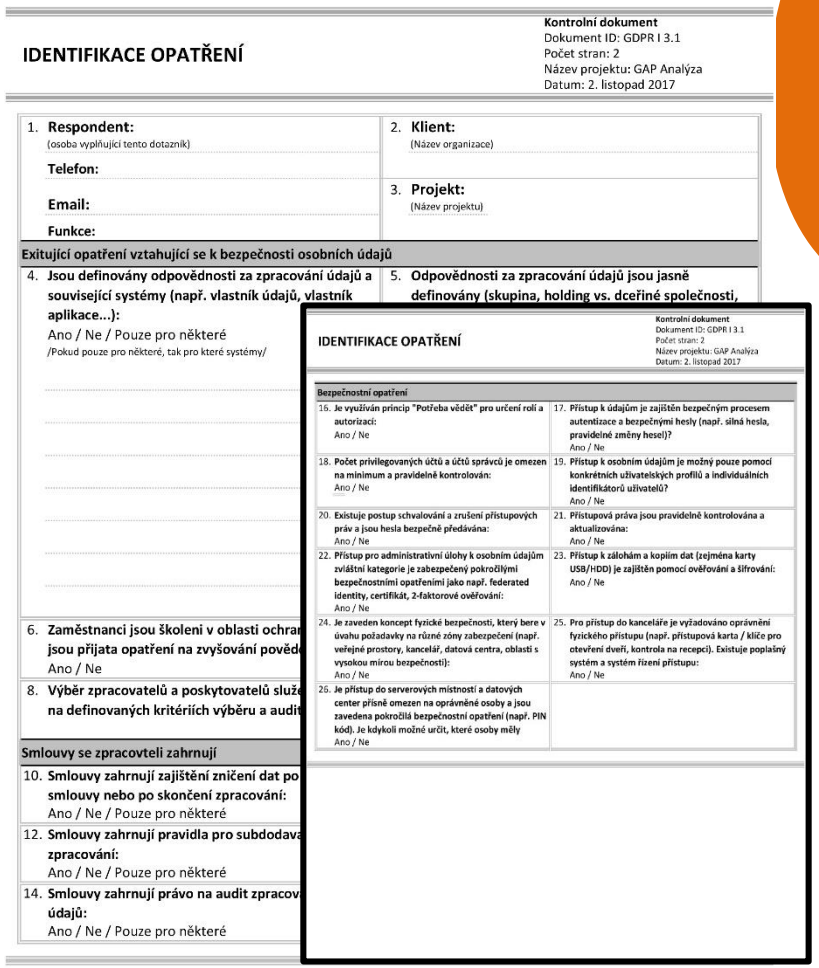
34. **Aplikace umožňuje export dat**
(Systém umožňuje export dat)
Ano / Ne
35. **Data z aplikace jsou odesílána mimo systém**
(Data ze systému jsou odesílána)
Ano / Ne

**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 ochran jsou přijata opatření na zvyšování pově**
Ano / Ne
8. **Výběr zpracovatelů a poskytovatelů služ 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**

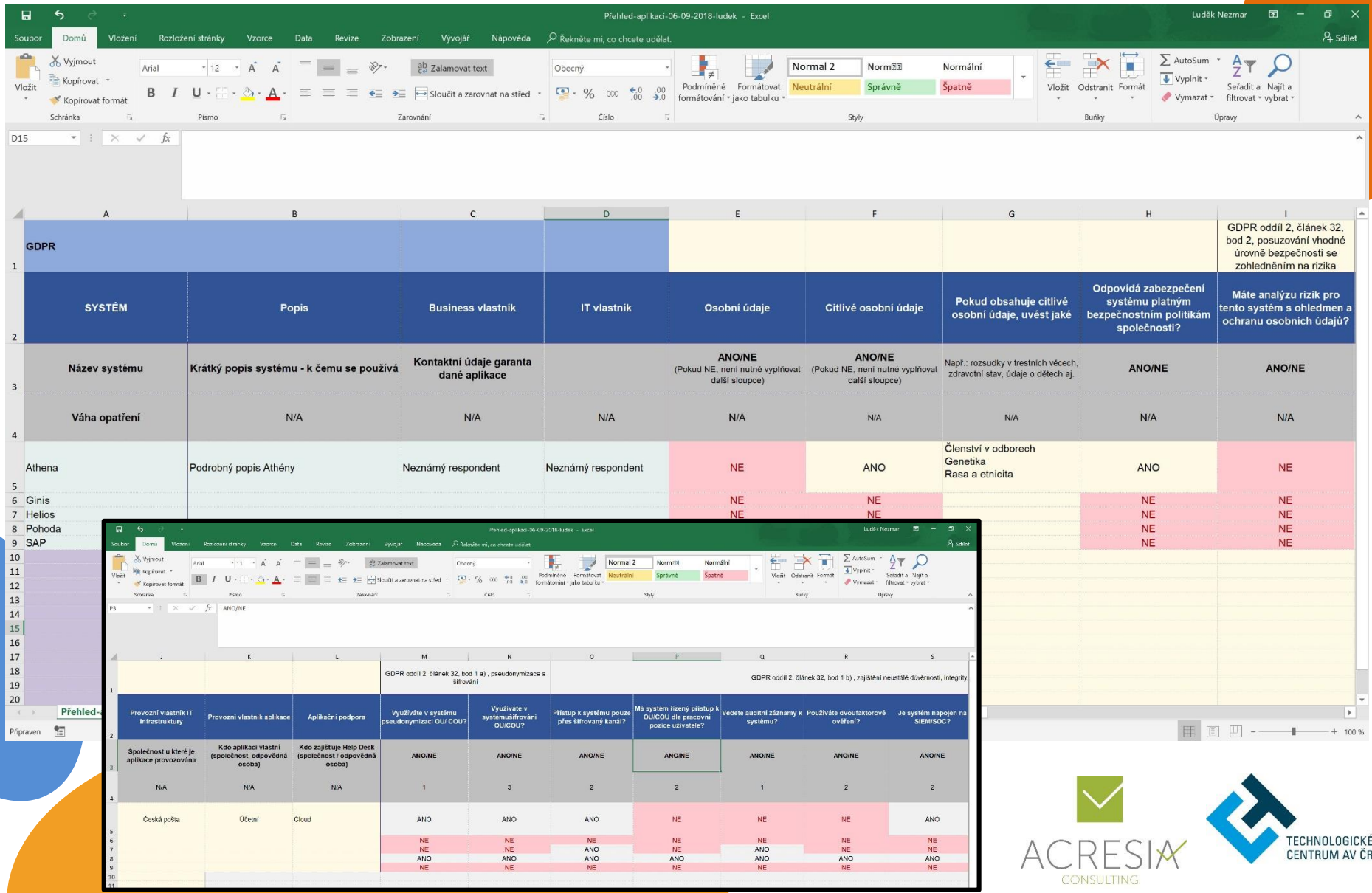
16. **Je využíván princip "Potřeba vědět" pro určení rolí a autorizaci:**
Ano / Ne
17. **Přístup k údajům je zajištěn bezpečným procesem autentizace a bezpečnými hesly (např. silná hesla, pravidelné změny hesel)?**
Ano / Ne
18. **Počet privilegovaných účtů a účtů správců je omezen na minimum a pravidelně 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

TECHNOLOGICKÉ CENTRUM AV ČR

# 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<br>Genetika<br>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 |



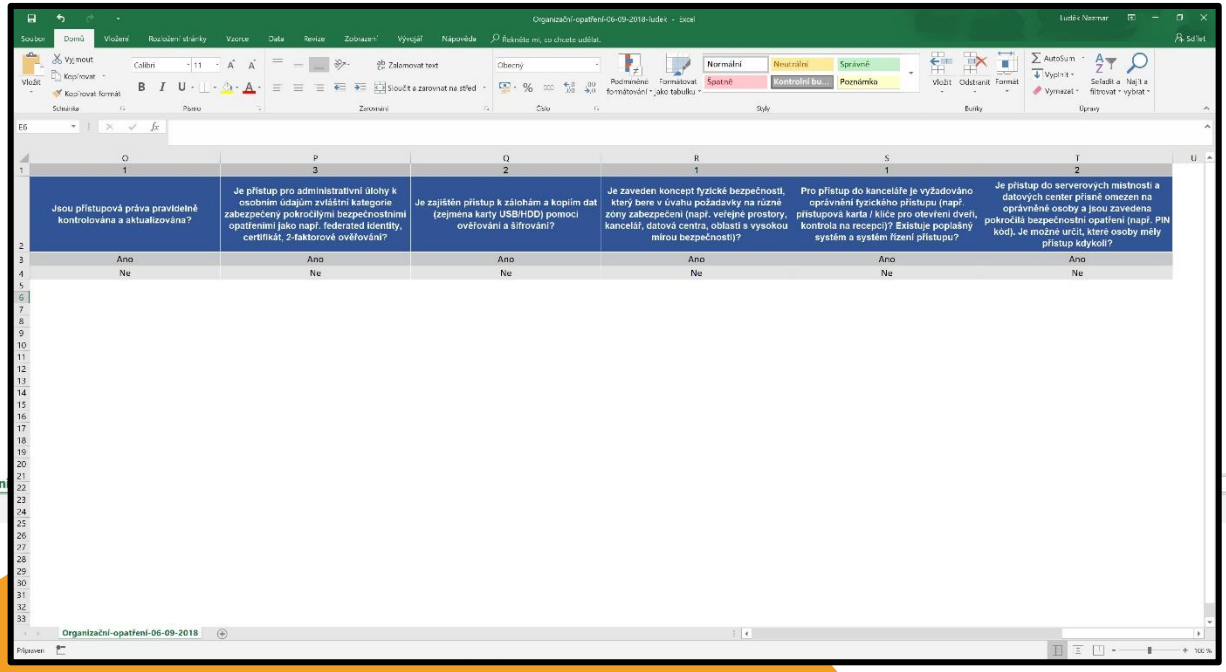
| | J | K | L | M | N | O | P | Q | R | S |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | GDPR oddíl 2, článek 32, bod 1 a) , pseudonymizace a šifrování | | | GDPR oddíl 2, článek 32, bod 1 b) , zajištění neustálé důvěrnosti, integrity, | | | |
| 2 | Provozní vlastník IT infrastruktury | Provozní vlastník aplikace | Aplikační podpora | Využíváte v systému pseudonymizaci OU/ COU? | Využíváte v systémusifrování 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 |
| 10 | | | | | | | | | | |
| 11 | | | | | | | | | | |

ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

# 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 |

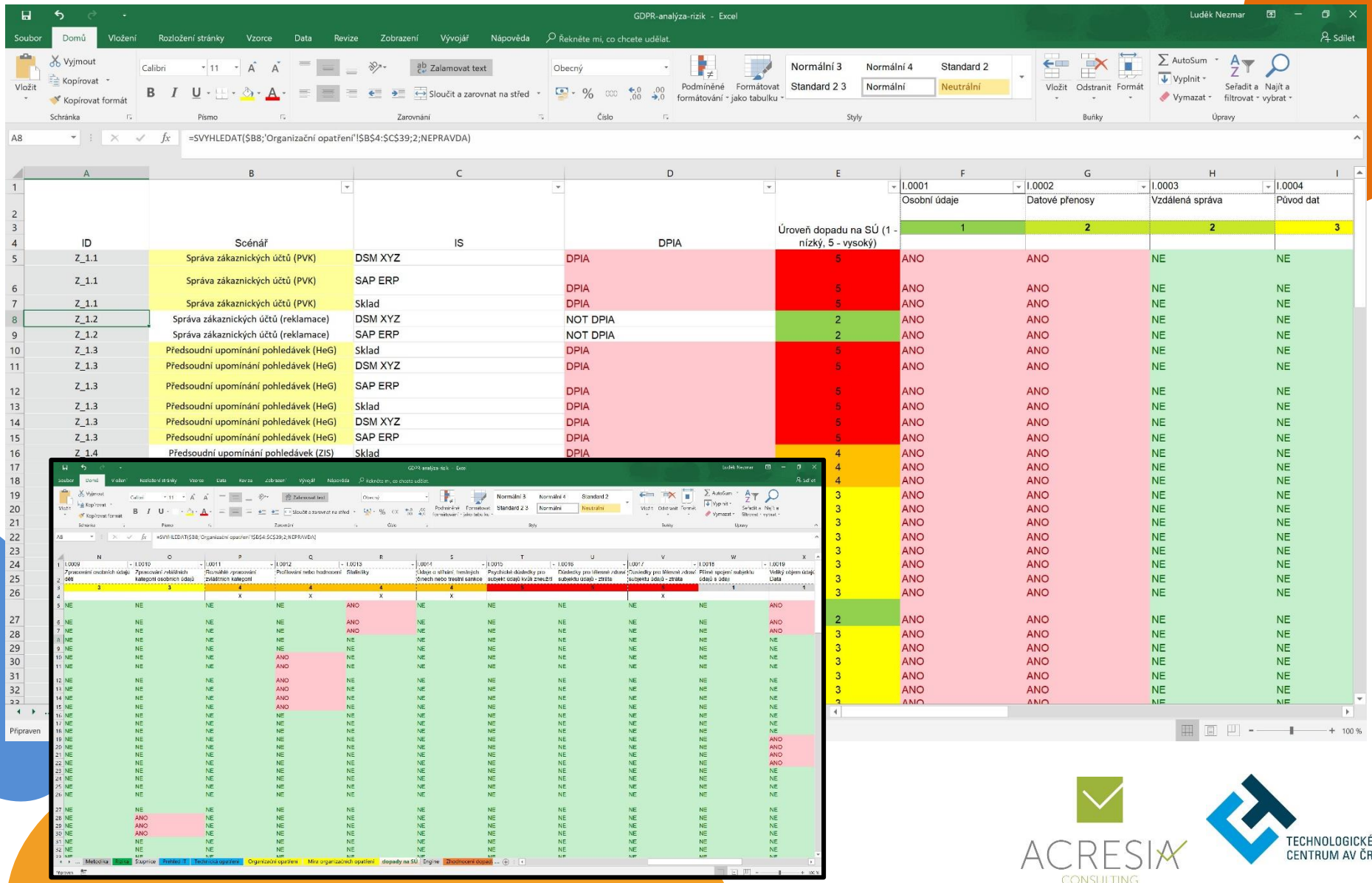


| | | | | | |
|---|---|---|---|---|---|
| 1 | 3 | 2 | 1 | 1 | 2 |
| Jsou přístupová práva pravidelně kontrolována a aktualizována? | Je přístup pro administrativní úlohy k osobním údajům zvláštní kategorie zabezpečený pokročilými bezpečnostními opatřeními jako např. federated identity, certifikát, 2-faktorové 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 poplašný 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? |
| Ano | Ano | Ano | Ano | Ano | Ano |
| Ne | Ne | Ne | Ne | Ne | Ne |

ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

# Analýza rizik – dopady na SÚ

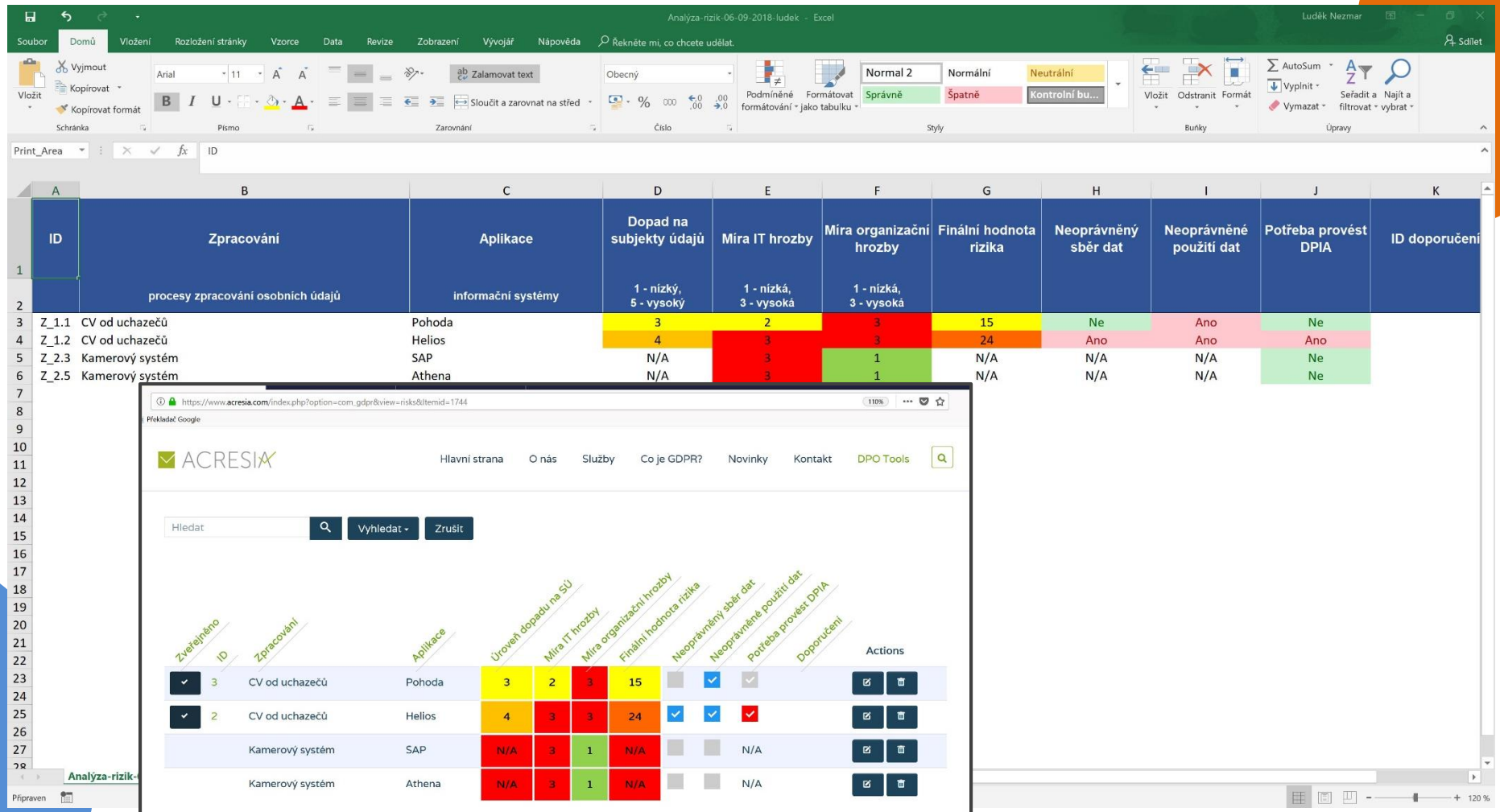


| ID | Scénář | IS | DPIA | Úroveň dopadu na SÚ (1 - nízký, 5 - vysoký) | I.0001 Osobní údaje | I.0002 Datové přenosy | I.0003 Vzdálená správa | I.0004 Původ dat |
|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 2 | 3 |
| Z_1.1 | Správa zákaznických účtů (PVK) | DSM XYZ | DPIA | 5 | ANO | ANO | 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 |

ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

# Analýza rizik – výsledek



| ID | Zpracování<br>procesy zpracování osobních údajů | Aplikace<br>informační systémy | Dopad na subjekty údajů<br>1 - nízký, 5 - vysoký | Míra IT hrozby<br>1 - nízká, 3 - vysoká | Míra organizační hrozby<br>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

TECHNOLOGICKÉ CENTRUM AV ČR

# Posuzování vlivu na ochranu osobních údajů

**Obsahem posouzení** musí být:

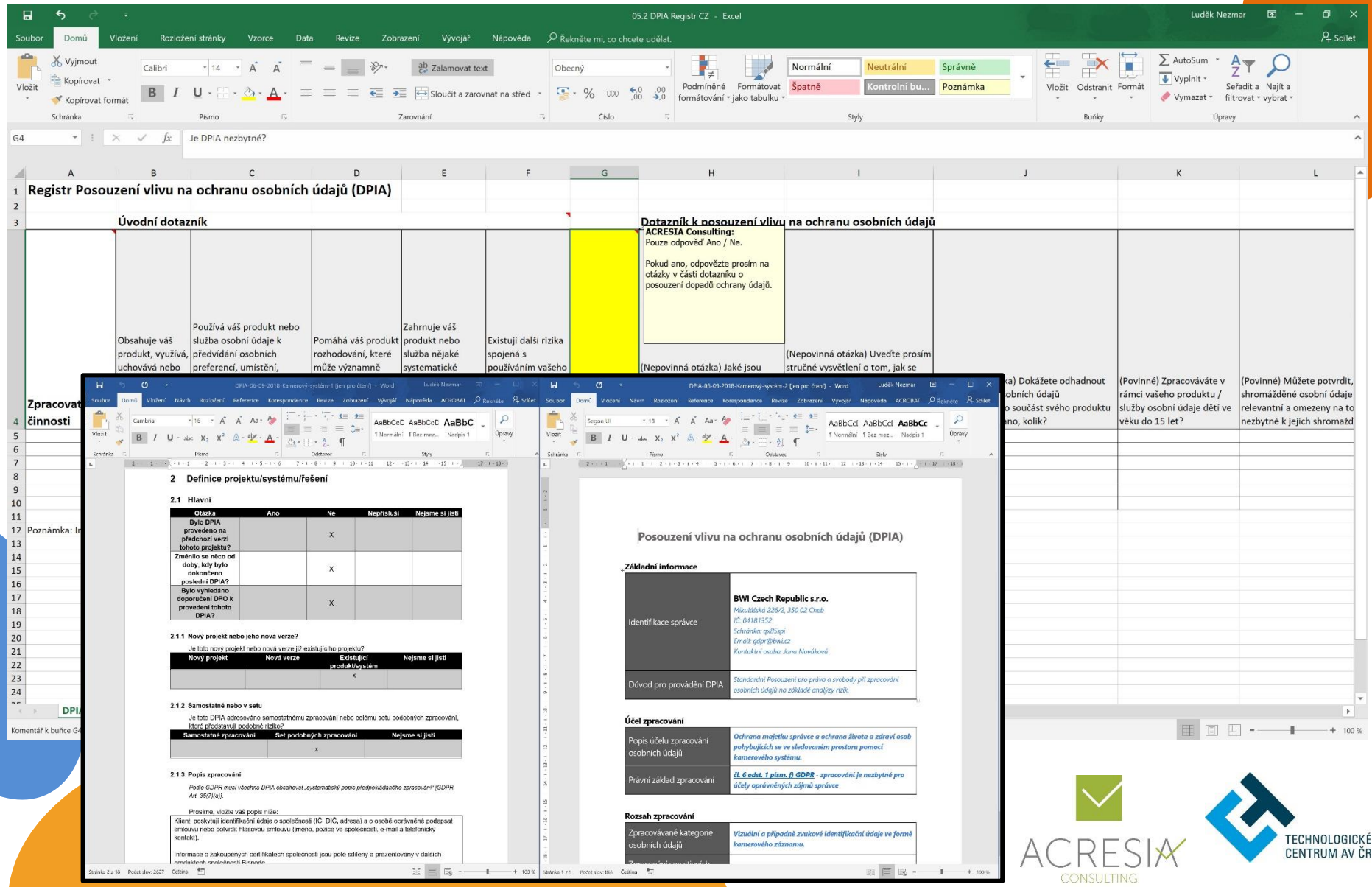
- Popis zamýšlených operací, účelů zpracování a oprávněných zájmů správce
- Zhodnocení nezbytnosti a proporcionality operací ve vztahu k účelům
- Zhodnocení rizika právům a svobodám jednotlivců
- Popis zamýšlených opatření ke zmírnění rizika, včetně bezpečnostních opatření a mechanismů

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

ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

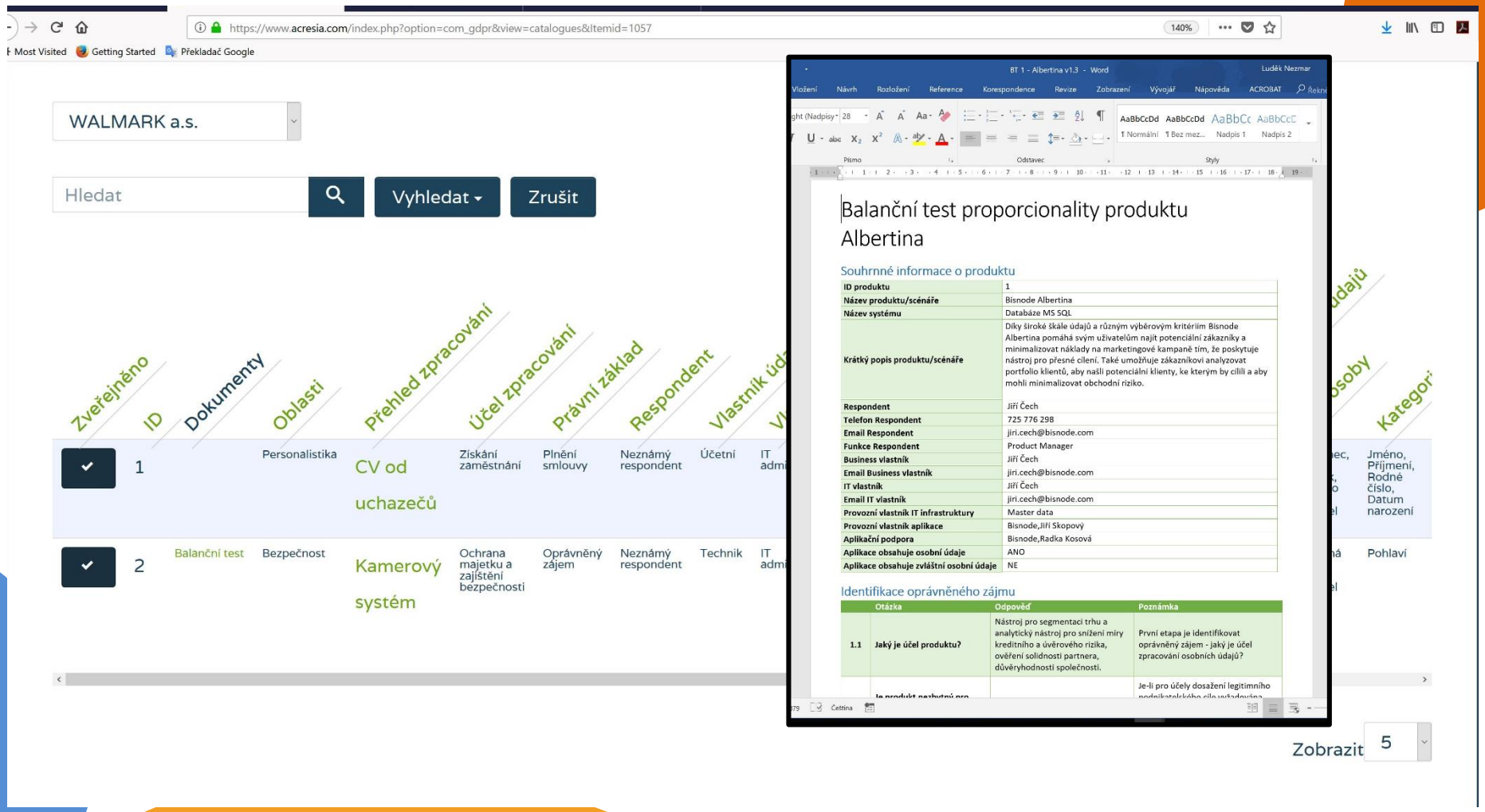
# Registr DPIA




ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

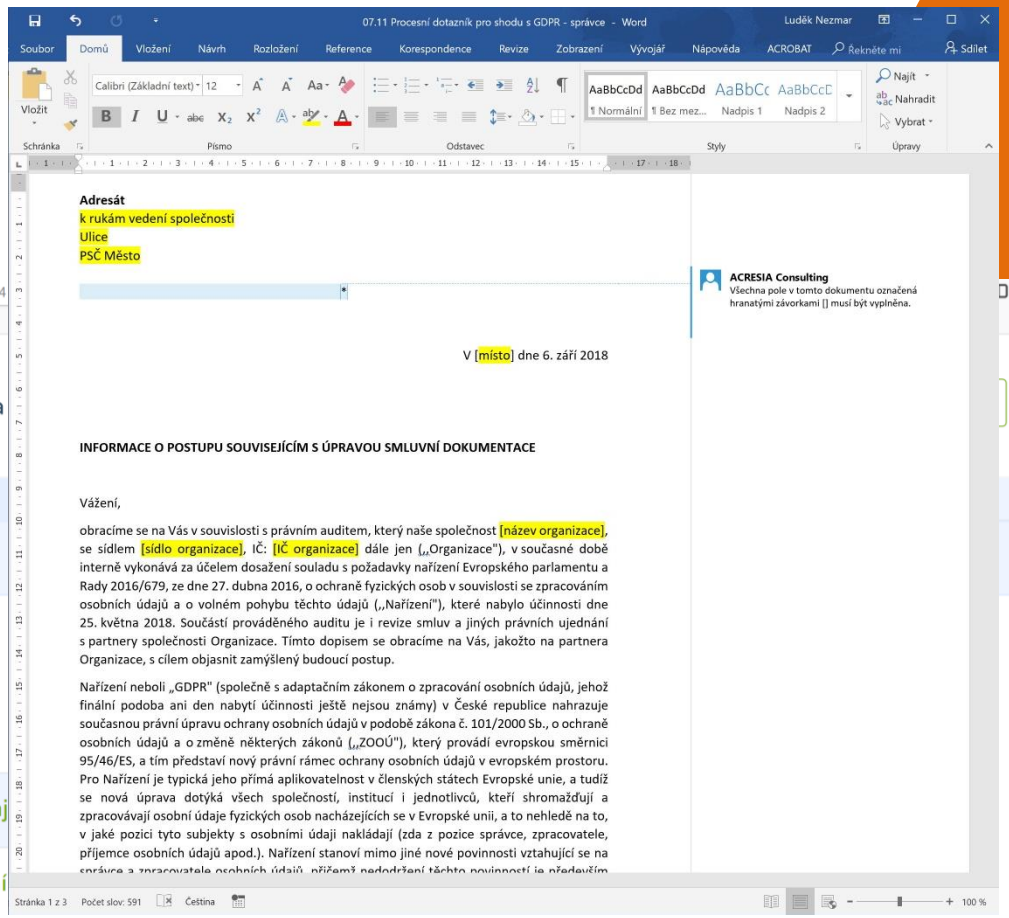
# Balanční test proporcionality




ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

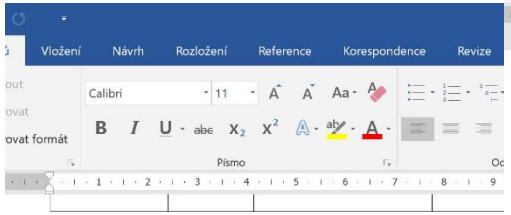
# Zpracovatelé




ACRESIA CONSULTING

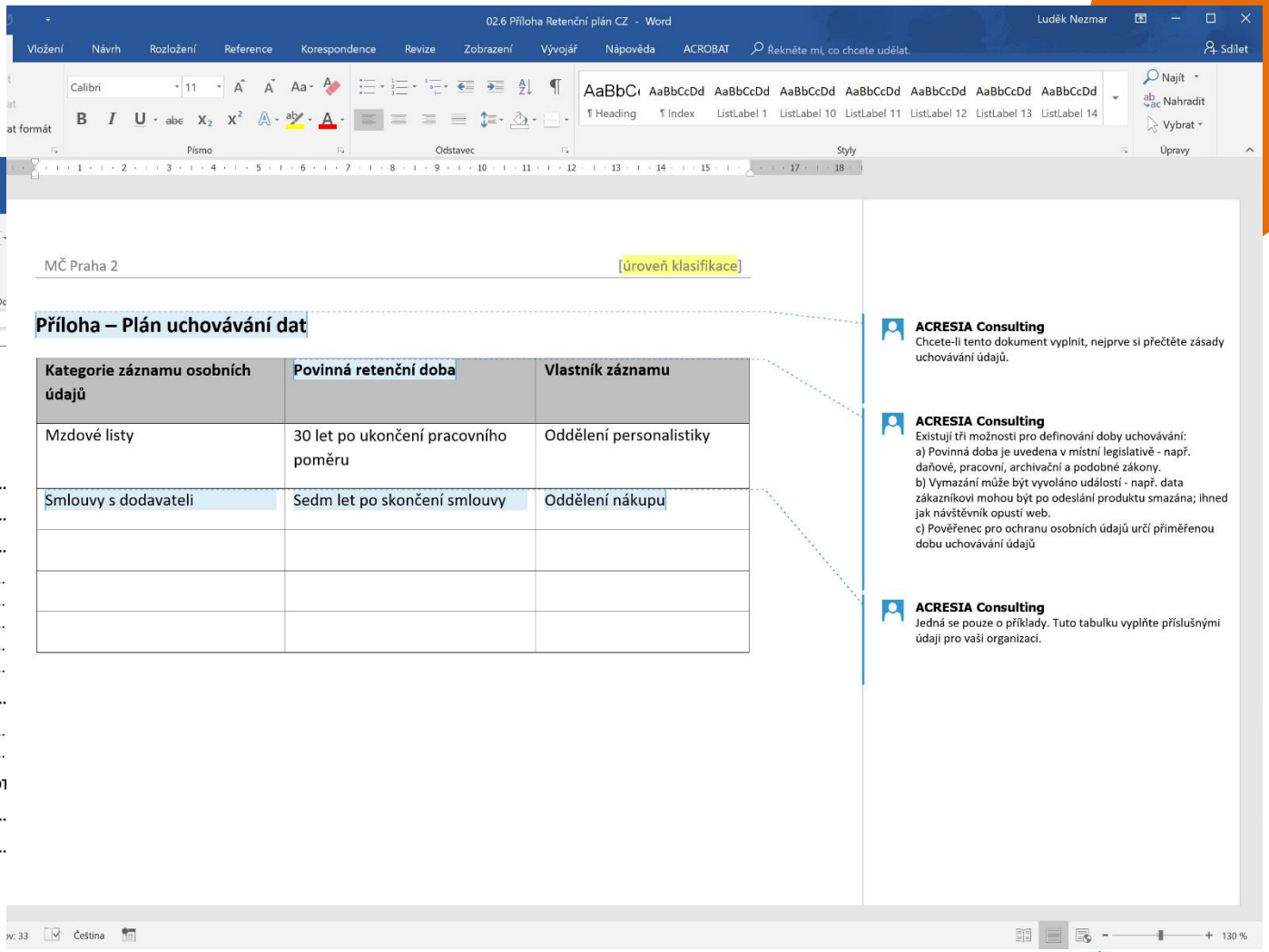
TECHNOLOGICKÉ CENTRUM AV ČR

# Retenční politika




## Obsah






ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

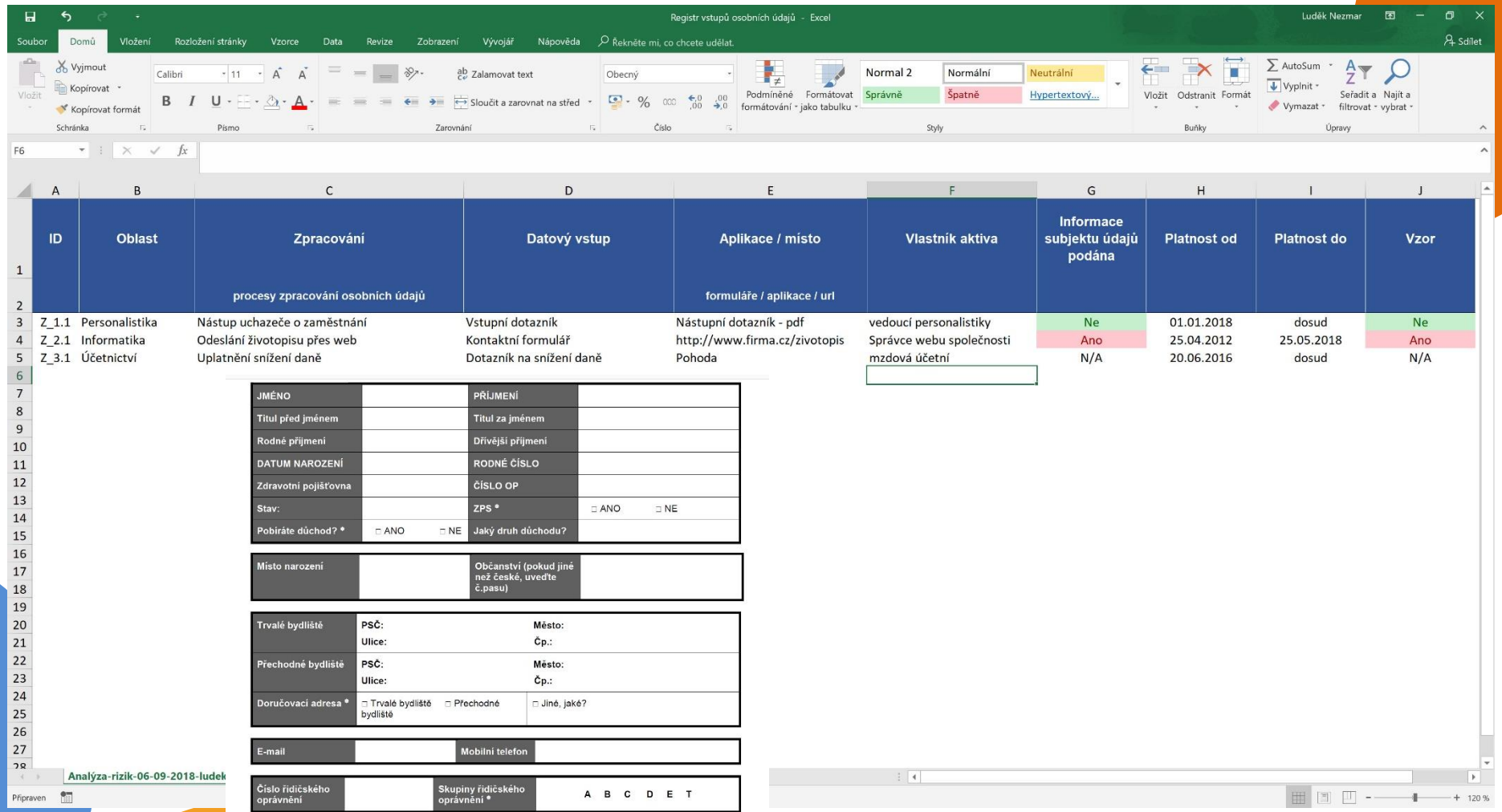
# Pověřenec - DPO

- 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

TECHNOLOGICKÉ CENTRUM AV ČR

# Registr vstupů osobních údajů




| ID | Oblast | Zpracování<br>procesy zpracování osobních údajů | Datový vstup | Aplikace / místo<br>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:<br>Ulice: | Město:<br>Čp.: | |
| Přechodné bydliště | PSČ:<br>Ulice: | Město:<br>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

TECHNOLOGICKÉ CENTRUM AV ČR

# 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), oznamovací povinnosti vůči příslušným úřadům

ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

# 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

TECHNOLOGICKÉ CENTRUM AV ČR

# GDPR dokumentace

ACRESIA CONSULTING

## 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), 1 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) |

ACRESIA CONSULTING

| Č. | Kód dokumentu | Název dokumentu | Odpovídající článek 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 | 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 |

ACRESIA CONSULTING

| Č. | Kód dokumentu | Název dokumentu | Odpovídající článek 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 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.

ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

# 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

ACRESIA CONSULTING

TECHNOLOGICKÉ CENTRUM AV ČR

# Na co dále nezapomenout

| | |
|---|---|
| Identifikace zpracování | • Určení účelů a titulů zpracování<br>• Určení podmínek zpracování |
| Pověřenec | • Vymezit činnosti, nasmlouvat jeho činnost<br>• 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

TECHNOLOGICKÉ CENTRUM AV ČR

# Děkuji za pozornost

www.acresia.com

ACRESIA
CONSULTING