# GDPR ve zdravotnictví

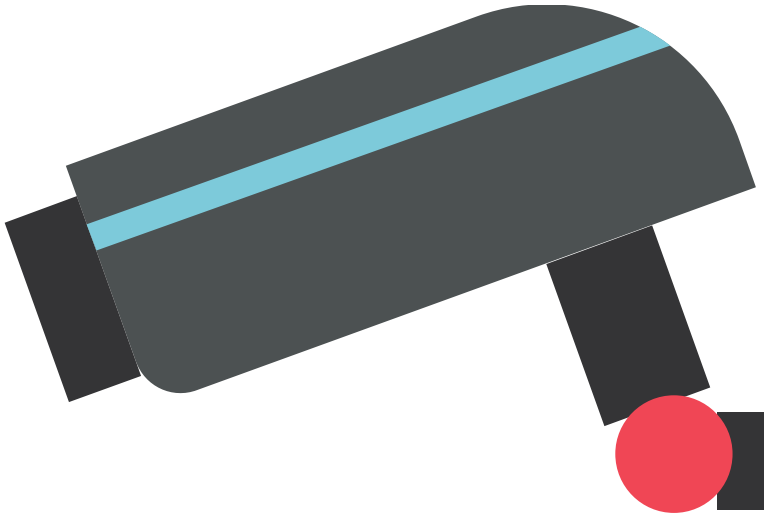
Mgr. Štěpán Holub

Praha, 12. 12. 2017

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 115 579, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

# Osobní údaje 2018

holubova.cz



**20 000 000 EUR**

4 % obratu

# GDPR

# General Data Protection Regulation
# Obecné nařízení o ochraně osobních údajů

# Evropská směrnice

- Směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
- Zákon č. 101/2000 Sb., o ochraně osobních údajů

# Evropské nařízení

- GDPR
- doprovodné zákony


25. května 2018

# Jak jednoduše dostat pokutu?

1. Budete ignorovat existenci GDPR
2. Do 72 hodin nenahlásíte únik osobních údajů
3. Neprokážete udělení souhlasu k jejich zpracování


SPAM
SUBMIT

# 4,25 mio CZK

# 3,6 mio CZK

# Zdravotnická dokumentace

# 60 000,- CZK

# Pokuty dle GDPR

1. Odrazující
2. Účinné
3. Přiměřené

„Obecné nařízení říká, že pokuty musí být odrazující. Tím se budeme řídit. Pokuty mohou být velmi velmi vysoké, doteď nebyly.“

*(Ivana Janů, předsedkyně ÚOOÚ, E15.cz ze dne 17.7.2017)*

# Na jaké zpracovávání se GDPR vztahuje?

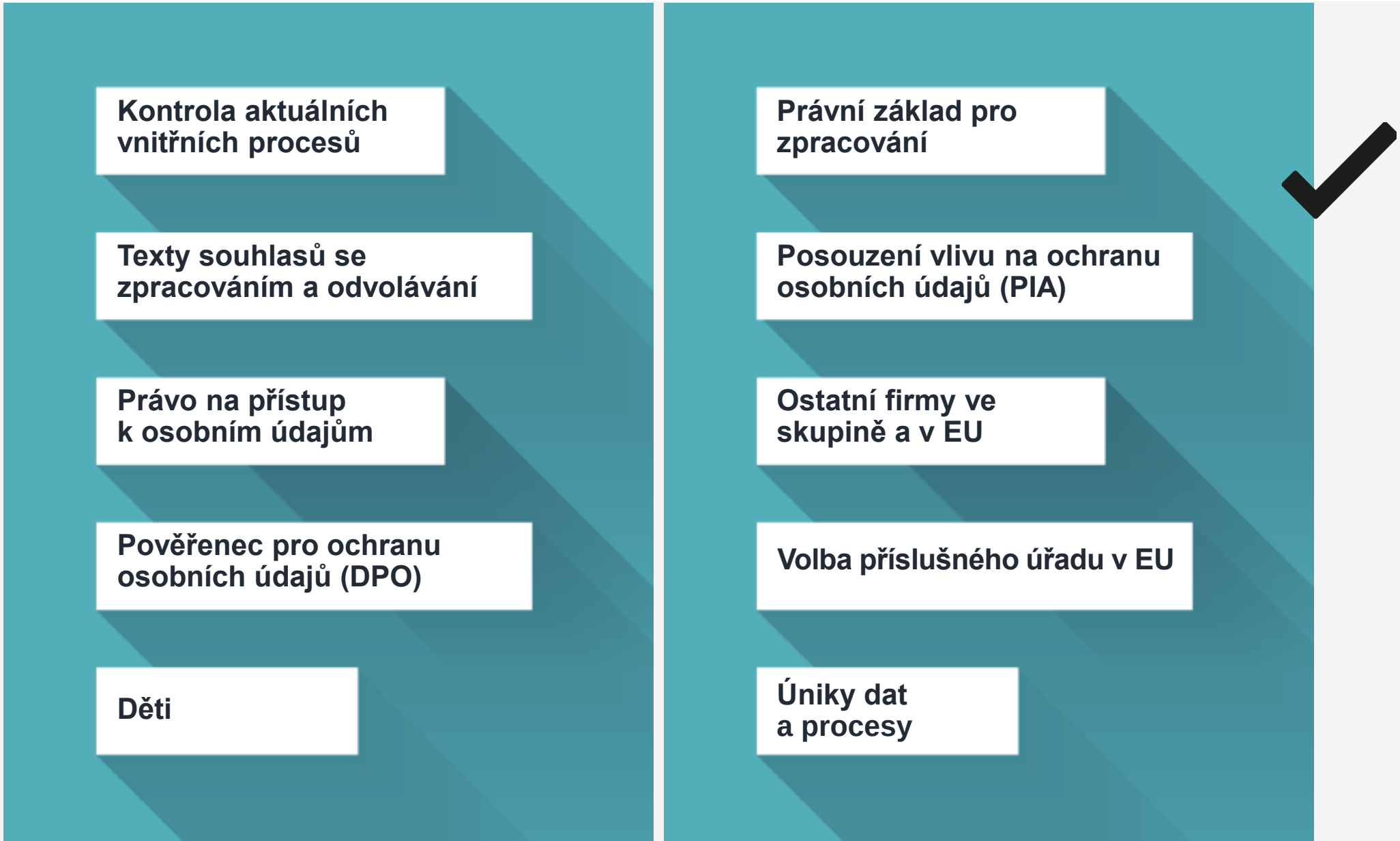
1. Automatické
2. Manuální

# Týká se GDPR Vás?

1. Zpracováváte osobní údaje pacientů? .....
2. Monitorujete veřejně přístupné prostory kamerami? .....
3. Sledujete auta zaměstnanců přes GPS? .....
4. Zpracováváte osobní data zaměstnanců? .....
5. Sbírá Váš software místa pohybu, osobní údaje, IP adresy? .....

# Příprava na GDPR …

holubova.cz



# Hrozby ve zdravotnictví

1. Rozsah údajů
2. Kritičnost údajů
3. Náchylnost k útoku

# Ransomware útok

# Tak postupně…

# Obsah přednášky

1. Základní pojmy GDPR
2. Právní důvody zpracování osobních údajů
3. Práva a povinnosti v GDPR
4. Zabezpečení osobních údajů
5. Nové povinnosti
6. Pověřenec pro ochranu osobních údajů a jiné specifické povinnosti správce
7. Shrnutí

# 1. Základní pojmy

# Osobní údaj

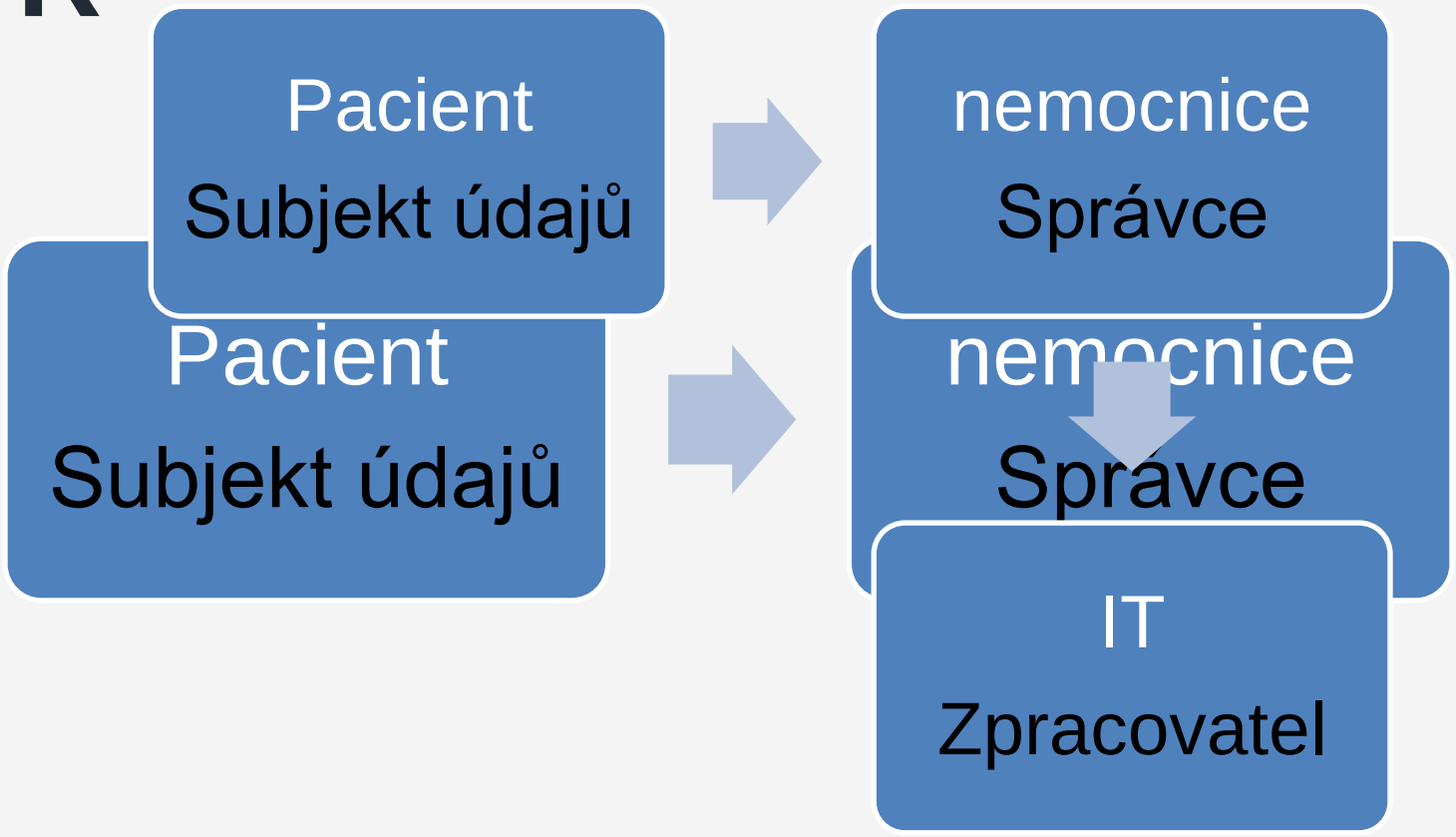
- jakákoliv informace o určené nebo určitelné fyzické osobě

# Zvláštní kategorie osobních údajů

1. Rasový či etnický původ
2. Politický názor
3. Náboženské vyznání
4. Filozofické přesvědčení
5. Členství v odborech
6. Genetické údaje zpracované za účelem jedinečné identifikace FO
7. Biometrické údaje zpracované za účelem jedinečné identifikace FO
8. **Zdravotní stav**
9. Sexuální život nebo sexuální orientace

# Osoby v GDPR

1. Subjekt údajů
2. Správce
3. Zpracovatel



# Zásady zpracování

1. Transparentnost
2. Vymezený účel
3. Minimalizace
4. Doba uložení
5. Zabezpečení

# Úkol 1

# 2. Právní důvody zpracování

# Právní důvody zpracování běžných OÚ

1. Smlouva
2. Zákon
3. Životně důležitý zájem
4. Veřejný zájem
5. Oprávněný zájem správce
6. Souhlas

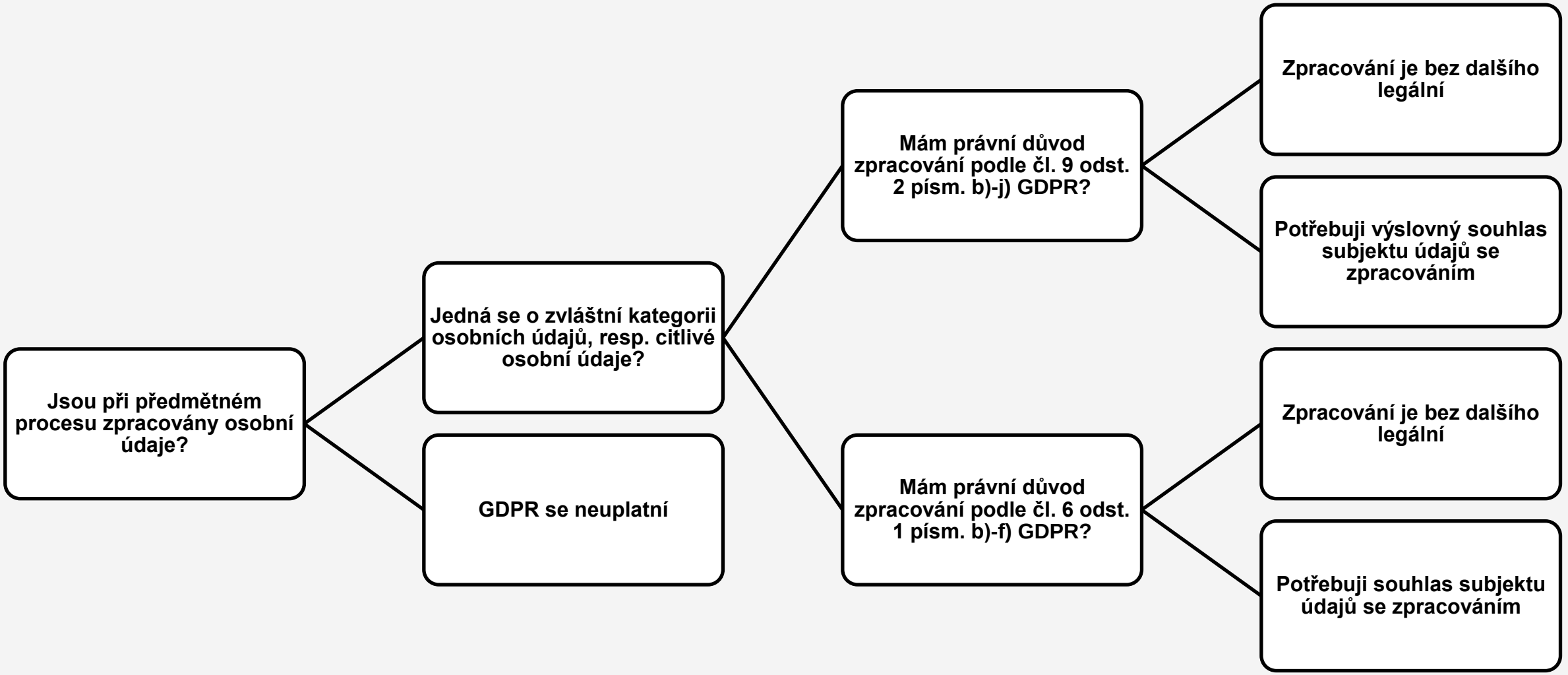
# I. Právní důvody zpracování citlivých OÚ

1. Výslovný souhlas
2. Nezbytné pro účely pracovního práva a sociálního zabezpečení
3. Ochrana životně důležitých zájmů
4. Zpracování prováděné nadací apod.
5. Údaje zjevně zveřejněné subjektem údajů

# II. Právní důvody zpracování citlivých

# OÚ

6. Nezbytné pro soudní řízení
7. Významný veřejný zájem
8. Preventivní, pracovní lékařství apod.
9. Veřejné zdraví
10. Archivace ve veřejném zájmů apod.


Jsou při předmětném procesu zpracovány osobní údaje?
Jedná se o zvláštní kategorii osobních údajů, resp. citlivé osobní údaje?
GDPR se neuplatní
Mám právní důvod zpracování podle čl. 9 odst. 2 písm. b)-j) GDPR?
Mám právní důvod zpracování podle čl. 6 odst. 1 písm. b)-f) GDPR?
Zpracování je bez dalšího legální
Potřebuji výslovný souhlas subjektu údajů se zpracováním
Zpracování je bez dalšího legální
Potřebuji souhlas subjektu údajů se zpracováním

# Vedení zdravotnická dokumentace

Soubor informací o zdravotním stavu pacienta, průběhu a výsledku poskytovaných služeb a o dalších významných okolnostech souvisejících se zdravotním stavem pacienta a s postupem při poskytování zdravotních služeb … (ust. § 53 a násl. ZZS)

Právním důvodem je zákon

# Souhlas

1. Náležitosti
2. Prokazatelnost
3. Odvolatelnost

# Souhlas

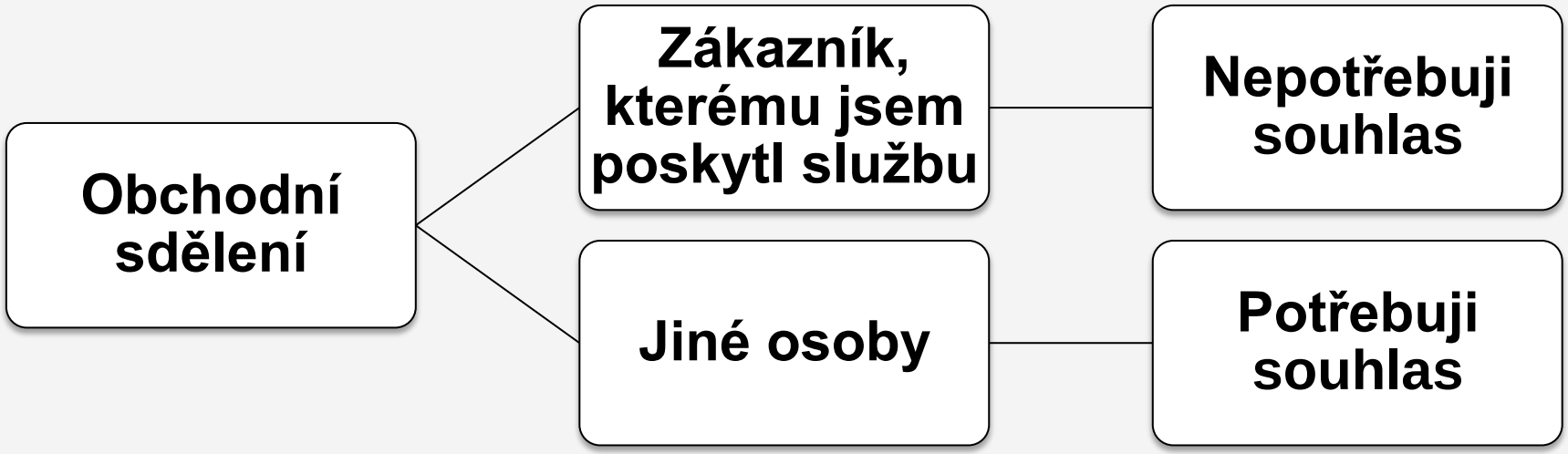
**informovaný**

- podle zákona o zdravotních službách
- podle občanského zákoníku
- podle Úmluvy o biomedicíně
- aj.

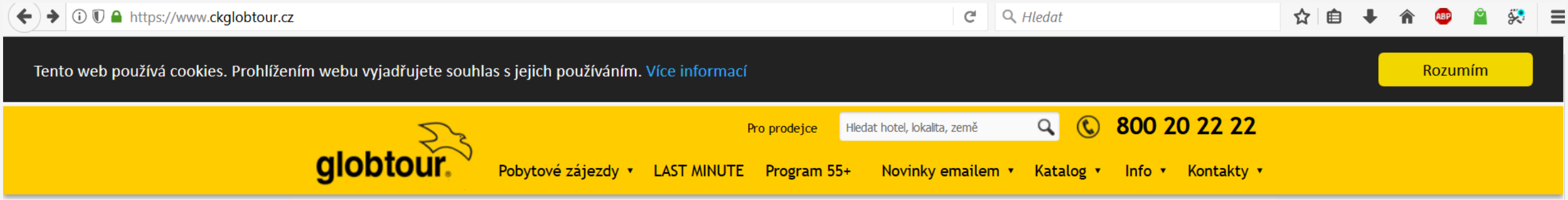
**se zpracováním osobních údajů**

- podle GDPR

# Zasílání obchodních sdělení



# Cookies


https://www.ckglobtour.cz
Hledat
Tento web používá cookies. Prohlížením webu vyjadřujete souhlas s jejich používáním. Více informací
Rozumím
Pro prodejce
Hledat hotel, lokalita, země
800 20 22 22
globtour
Pobytové zájezdy
LAST MINUTE
Program 55+
Novinky emailem
Katalog
Info
Kontakty

# Úkol 2

# 3. Práva a povinnosti v GDPR

# Ukládání a nakládání s osobními údaji

1. Zabezpečení
2. Úložiště v EU a mimo EU
3. Předávání

# I. Předávání osobních údajů

1. Ze zákona: Národní zdravotní informační systém
2. Jiný základ: předání jinému lékaři jako podklad pro studii

# II. Předávání osobních údajů

1. V rámci EU
2. Mimo EU

1. Transparentnost

1. Transparentnost
2. Zabezpečení
3. Poučení o (ne)existenci rozhodnutí EK

# Práva uživatele

1. Informace o zpracovávaných údajích
2. Přenositelnost
3. Právo být zapomenut
4. Rozhodování dle profilování
5. Poučování

# Požadavky na informační systém

# Software zdravotnických přístrojů

1. Součást zdravotnické dokumentace
2. Výmaz osobních údajů
3. Zabezpečení

# Úkol 3

# 4. Zabezpečení

# Hlediska vhodného zabezpečení

1. stav techniky
2. náklady na provedení
3. povaha, rozsah, kontext a účel zpracování
4. pravděpodobnost a závažnost rizika

# Zabezpečení musí odpovídat riziku!

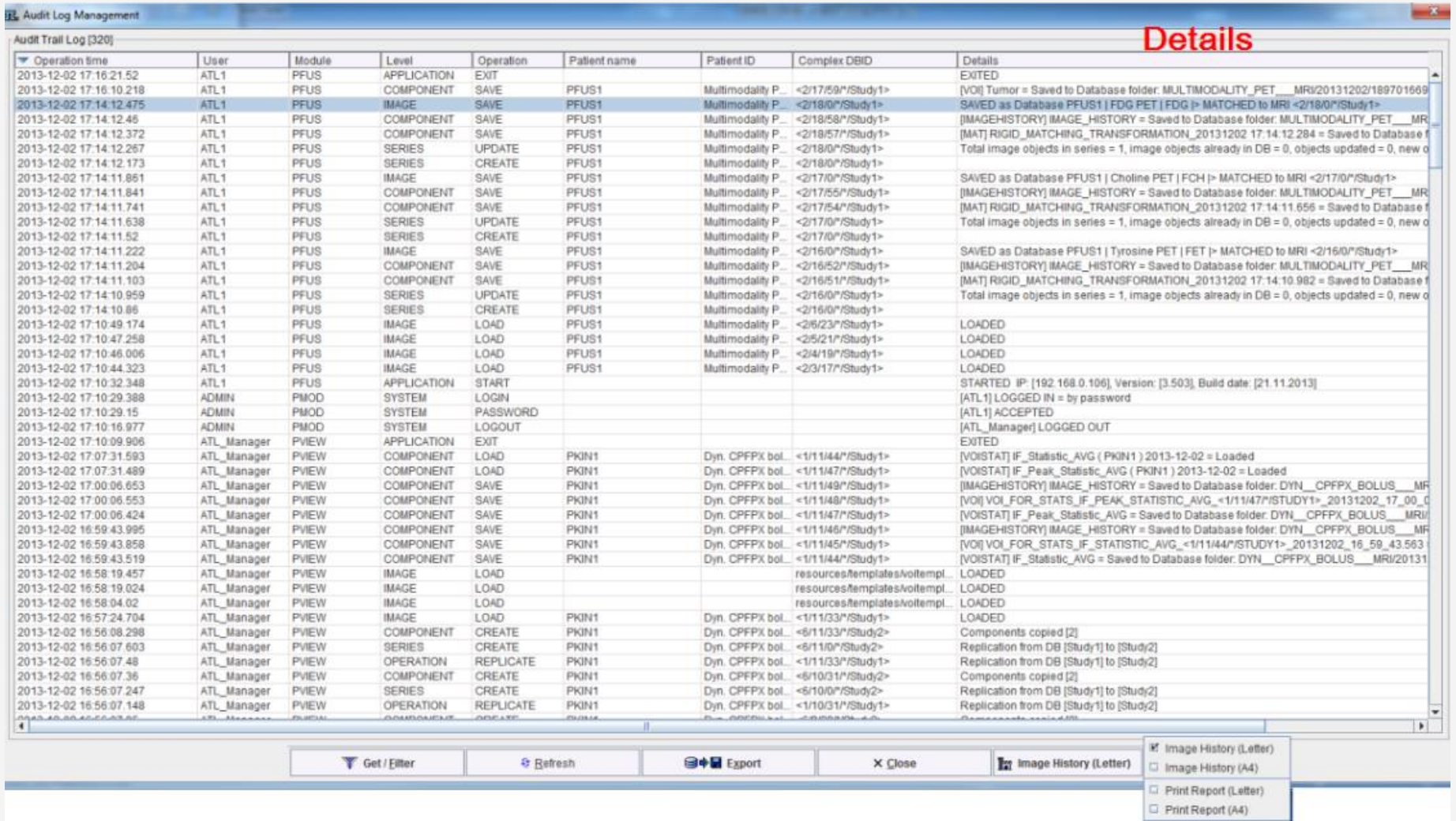

» SECURITY «


Password:
**********

# Doporučené způsoby zabezpečení dat

1. Anonymizace
2. Pseudonymizace
3. Šifrování

# Audit Trail


Audit Log Management
Audit Trail Log [320]
Details
Operation time | User | Module | Level | Operation | Patient name | Patient ID | Complex DBID | Details
2013-12-02 17:16:21.52 | ATL1 | PFUS | APPLICATION | EXIT | | | | EXITED
2013-12-02 17:16:10.218 | ATL1 | PFUS | COMPONENT | SAVE | PFUS1 | Multimodality P... | <2/17/59/*/Study1> | [VOI] Tumor = Saved to Database folder: MULTIMODALITY_PET___MRI/20131202/189701669
2013-12-02 17:14:12.475 | ATL1 | PFUS | IMAGE | SAVE | PFUS1 | Multimodality P... | <2/18/0/*/Study1> | SAVED as Database PFUS1 | FDG PET | FDG |> MATCHED to MRI <2/18/0/*/Study1>
2013-12-02 17:14:12.46 | ATL1 | PFUS | COMPONENT | SAVE | PFUS1 | Multimodality P... | <2/18/58/*/Study1> | [IMAGEHISTORY] IMAGE_HISTORY = Saved to Database folder: MULTIMODALITY_PET___MR
2013-12-02 17:14:12.372 | ATL1 | PFUS | COMPONENT | SAVE | PFUS1 | Multimodality P... | <2/18/57/*/Study1> | [MAT] RIGID_MATCHING_TRANSFORMATION_20131202 17:14:12.284 = Saved to Database f
2013-12-02 17:14:12.267 | ATL1 | PFUS | SERIES | UPDATE | PFUS1 | Multimodality P... | <2/18/0/*/Study1> | Total image objects in series = 1, image objects already in DB = 0, objects updated = 0, new o
2013-12-02 17:14:12.173 | ATL1 | PFUS | SERIES | CREATE | PFUS1 | Multimodality P... | <2/18/0/*/Study1> |
2013-12-02 17:14:11.861 | ATL1 | PFUS | IMAGE | SAVE | PFUS1 | Multimodality P... | <2/17/0/*/Study1> | SAVED as Database PFUS1 | Choline PET | FCH |> MATCHED to MRI <2/17/0/*/Study1>
2013-12-02 17:14:11.841 | ATL1 | PFUS | COMPONENT | SAVE | PFUS1 | Multimodality P... | <2/17/55/*/Study1> | [IMAGEHISTORY] IMAGE_HISTORY = Saved to Database folder: MULTIMODALITY_PET___MR
2013-12-02 17:14:11.741 | ATL1 | PFUS | COMPONENT | SAVE | PFUS1 | Multimodality P... | <2/17/54/*/Study1> | [MAT] RIGID_MATCHING_TRANSFORMATION_20131202 17:14:11.656 = Saved to Database f
2013-12-02 17:14:11.638 | ATL1 | PFUS | SERIES | UPDATE | PFUS1 | Multimodality P... | <2/17/0/*/Study1> | Total image objects in series = 1, image objects already in DB = 0, objects updated = 0, new o
2013-12-02 17:14:11.52 | ATL1 | PFUS | SERIES | CREATE | PFUS1 | Multimodality P... | <2/17/0/*/Study1> |
2013-12-02 17:14:11.222 | ATL1 | PFUS | IMAGE | SAVE | PFUS1 | Multimodality P... | <2/16/0/*/Study1> | SAVED as Database PFUS1 | Tyrosine PET | FET |> MATCHED to MRI <2/16/0/*/Study1>
2013-12-02 17:14:11.204 | ATL1 | PFUS | COMPONENT | SAVE | PFUS1 | Multimodality P... | <2/16/52/*/Study1> | [IMAGEHISTORY] IMAGE_HISTORY = Saved to Database folder: MULTIMODALITY_PET___MR
2013-12-02 17:14:11.103 | ATL1 | PFUS | COMPONENT | SAVE | PFUS1 | Multimodality P... | <2/16/51/*/Study1> | [MAT] RIGID_MATCHING_TRANSFORMATION_20131202 17:14:10.982 = Saved to Database f
2013-12-02 17:14:10.959 | ATL1 | PFUS | SERIES | UPDATE | PFUS1 | Multimodality P... | <2/16/0/*/Study1> | Total image objects in series = 1, image objects already in DB = 0, objects updated = 0, new o
2013-12-02 17:14:10.86 | ATL1 | PFUS | SERIES | CREATE | PFUS1 | Multimodality P... | <2/16/0/*/Study1> |
2013-12-02 17:10:49.174 | ATL1 | PFUS | IMAGE | LOAD | PFUS1 | Multimodality P... | <2/6/23/*/Study1> | LOADED
2013-12-02 17:10:47.258 | ATL1 | PFUS | IMAGE | LOAD | PFUS1 | Multimodality P... | <2/5/21/*/Study1> | LOADED
2013-12-02 17:10:46.006 | ATL1 | PFUS | IMAGE | LOAD | PFUS1 | Multimodality P... | <2/4/19/*/Study1> | LOADED
2013-12-02 17:10:44.323 | ATL1 | PFUS | IMAGE | LOAD | PFUS1 | Multimodality P... | <2/3/17/*/Study1> | LOADED
2013-12-02 17:10:32.348 | ATL1 | PFUS | APPLICATION | START | | | | STARTED IP: [192.168.0.106], Version: [3.503], Build date: [21.11.2013]
2013-12-02 17:10:29.388 | ADMIN | PMOD | SYSTEM | LOGIN | | | | [ATL1] LOGGED IN = by password
2013-12-02 17:10:29.15 | ADMIN | PMOD | SYSTEM | PASSWORD | | | | [ATL1] ACCEPTED
2013-12-02 17:10:16.977 | ADMIN | PMOD | SYSTEM | LOGOUT | | | | [ATL_Manager] LOGGED OUT
2013-12-02 17:10:09.906 | ATL_Manager | PVIEW | APPLICATION | EXIT | | | | EXITED
2013-12-02 17:07:31.593 | ATL_Manager | PVIEW | COMPONENT | LOAD | PKIN1 | Dyn. CPFPX bol... | <1/11/44/*/Study1> | [VOISTAT] IF_Statistic_AVG ( PKIN1 ) 2013-12-02 = Loaded
2013-12-02 17:07:31.489 | ATL_Manager | PVIEW | COMPONENT | LOAD | PKIN1 | Dyn. CPFPX bol... | <1/11/47/*/Study1> | [VOISTAT] IF_Peak_Statistic_AVG ( PKIN1 ) 2013-12-02 = Loaded
2013-12-02 17:00:06.653 | ATL_Manager | PVIEW | COMPONENT | SAVE | PKIN1 | Dyn. CPFPX bol... | <1/11/49/*/Study1> | [IMAGEHISTORY] IMAGE_HISTORY = Saved to Database folder: DYN__CPFPX_BOLUS___MR
2013-12-02 17:00:06.553 | ATL_Manager | PVIEW | COMPONENT | SAVE | PKIN1 | Dyn. CPFPX bol... | <1/11/48/*/Study1> | [VOI] VOI_FOR_STATS_IF_PEAK_STATISTIC_AVG_<1/11/47/*/STUDY1>_20131202_17_00_0
2013-12-02 17:00:06.424 | ATL_Manager | PVIEW | COMPONENT | SAVE | PKIN1 | Dyn. CPFPX bol... | <1/11/47/*/Study1> | [VOISTAT] IF_Peak_Statistic_AVG = Saved to Database folder: DYN__CPFPX_BOLUS___MRI/
2013-12-02 16:59:43.995 | ATL_Manager | PVIEW | COMPONENT | SAVE | PKIN1 | Dyn. CPFPX bol... | <1/11/46/*/Study1> | [IMAGEHISTORY] IMAGE_HISTORY = Saved to Database folder: DYN__CPFPX_BOLUS___MR
2013-12-02 16:59:43.858 | ATL_Manager | PVIEW | COMPONENT | SAVE | PKIN1 | Dyn. CPFPX bol... | <1/11/45/*/Study1> | [VOI] VOI_FOR_STATS_IF_STATISTIC_AVG_<1/11/44/*/STUDY1>_20131202_16_59_43.563
2013-12-02 16:59:43.519 | ATL_Manager | PVIEW | COMPONENT | SAVE | PKIN1 | Dyn. CPFPX bol... | <1/11/44/*/Study1> | [VOISTAT] IF_Statistic_AVG = Saved to Database folder: DYN__CPFPX_BOLUS___MRI/20131
2013-12-02 16:58:19.457 | ATL_Manager | PVIEW | IMAGE | LOAD | | | resources/templates/voitempl... | LOADED
2013-12-02 16:58:19.024 | ATL_Manager | PVIEW | IMAGE | LOAD | | | resources/templates/voitempl... | LOADED
2013-12-02 16:58:04.02 | ATL_Manager | PVIEW | IMAGE | LOAD | | | resources/templates/voitempl... | LOADED
2013-12-02 16:57:24.704 | ATL_Manager | PVIEW | IMAGE | LOAD | PKIN1 | Dyn. CPFPX bol... | <1/11/33/*/Study1> | LOADED
2013-12-02 16:56:08.298 | ATL_Manager | PVIEW | COMPONENT | CREATE | PKIN1 | Dyn. CPFPX bol... | <6/11/33/*/Study2> | Components copied [2]
2013-12-02 16:56:07.603 | ATL_Manager | PVIEW | SERIES | CREATE | PKIN1 | Dyn. CPFPX bol... | <6/11/0/*/Study2> | Replication from DB [Study1] to [Study2]
2013-12-02 16:56:07.48 | ATL_Manager | PVIEW | OPERATION | REPLICATE | PKIN1 | Dyn. CPFPX bol... | <1/11/33/*/Study1> | Replication from DB [Study1] to [Study2]
2013-12-02 16:56:07.36 | ATL_Manager | PVIEW | COMPONENT | CREATE | PKIN1 | Dyn. CPFPX bol... | <6/10/31/*/Study2> | Components copied [2]
2013-12-02 16:56:07.247 | ATL_Manager | PVIEW | SERIES | CREATE | PKIN1 | Dyn. CPFPX bol... | <6/10/0/*/Study2> | Replication from DB [Study1] to [Study2]
2013-12-02 16:56:07.148 | ATL_Manager | PVIEW | OPERATION | REPLICATE | PKIN1 | Dyn. CPFPX bol... | <1/10/31/*/Study1> | Replication from DB [Study1] to [Study2]
Get / Filter
Refresh
Export
Close
Image History (Letter)
Image History (Letter)
Image History (A4)
Print Report (Letter)
Print Report (A4)

# Sledování aktivity uživatelů

1. Monitoring aktivit uživatelů – PC, mobily, aplikace
2. Monitoring komunikace – email, FTP, web upload, screenshots, …

# Takto ne!


My
password
123456
End

# Ve zkratce

1. Fyzická ochrana datového centra, papírových dokumentů, monitoring tisku
2. Pravidelné update systémů, antiviry, firewalls, honeypots, ...
3. Zálohy dat ze serverů, PC, mobilních zařízení
4. Zajištění dostupnost pomocí duplikace systémů, monitoringu
5. Autentizace a autorizace uživatelů IS
6. Šifrovaná komunikace mezi systémy, vzájemná autentizace systémů
7. Data uložena na bezpečných místech (šifrování)
8. Pozor na USB disky, mobilní zařízení, emailovou komunikaci

# Úkol 4

# 5. Nové povinnosti

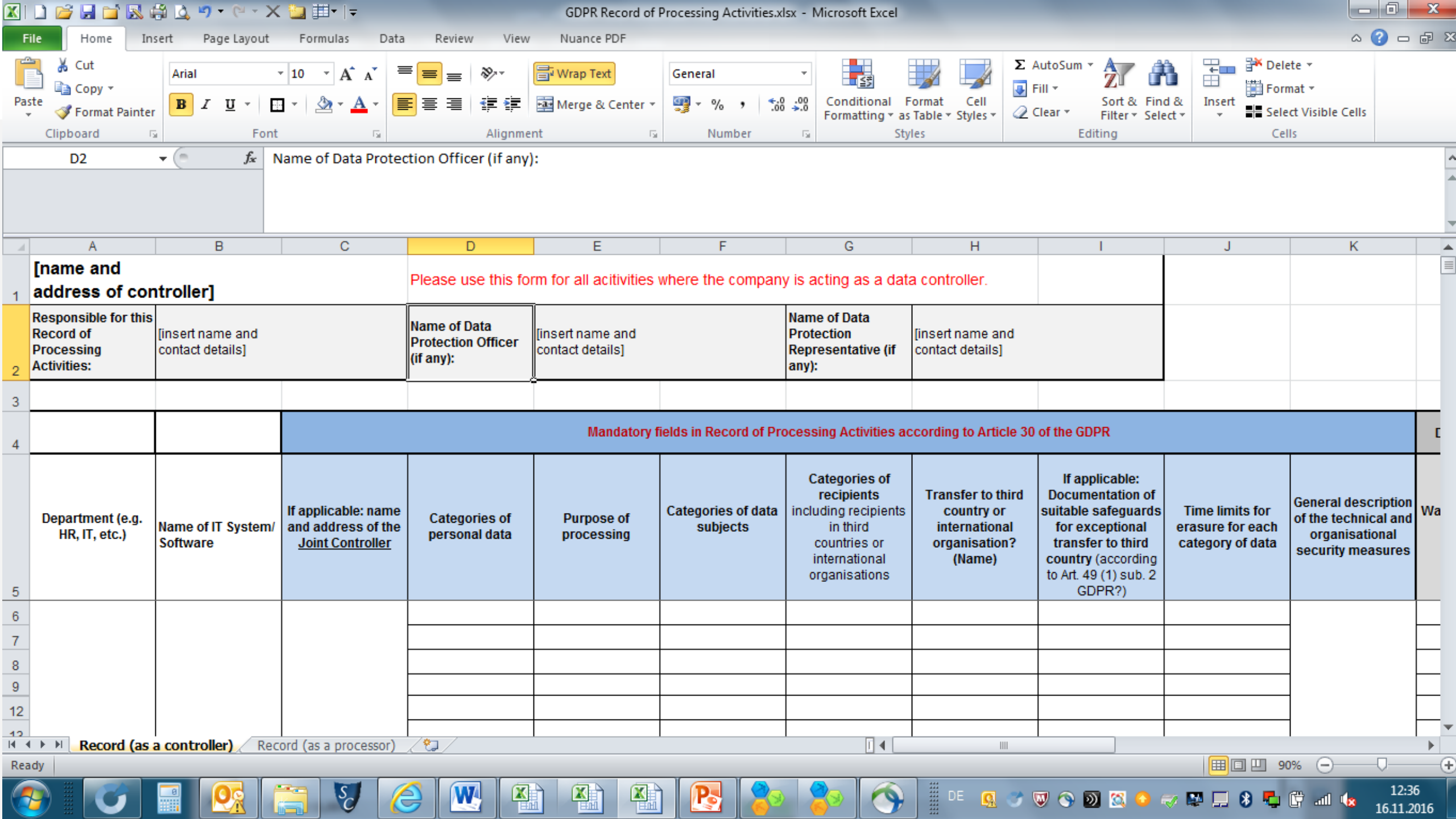
# I. Záznamy o činnostech zpracování

**Všichni vyjma**

- Méně než 250 zaměstnanců
  + zpracování je příležitostné
  + zpracování nepředstavuje riziko pro práva a svobody
  + zpracování nezahrnuje zvláštní kategorii osobních údajů

# II. Záznamy o činnostech zpracování

- Jméno + kontaktní údaje správce
- Účely zpracování
- Popis kategorií subjektu údajů a oú
- Kategorie příjemců
- Předání do třetí země
- Lhůta pro výmaz
- Technické a organizační bezpečnostní opatření



GDPR Record of Processing Activities.xlsx - Microsoft Excel

File | Home | Insert | Page Layout | Formulas | Data | Review | View | Nuance PDF

Cut | Copy | Format Painter | Paste | Clipboard
Arial | 10 | Font
Wrap Text | Merge & Center | Alignment
General | Number
Conditional Formatting | Format as Table | Cell Styles | Styles
AutoSum | Fill | Clear | Sort & Filter | Find & Select | Editing
Insert | Delete | Format | Select Visible Cells | Cells

D2: Name of Data Protection Officer (if any):

| | A | B | C | D | E | F | G | H | I | J | K |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **[name and address of controller]** | | | Please use this form for all acitivities where the company is acting as a data controller. | | | | | | | |
| 2 | **Responsible for this Record of Processing Activities:** | [insert name and contact details] | | **Name of Data Protection Officer (if any):** | [insert name and contact details] | | **Name of Data Protection Representative (if any):** | [insert name and contact details] | | | |
| 3 | | | | | | | | | | | |
| 4 | | | Mandatory fields in Record of Processing Activities according to Article 30 of the GDPR | | | | | | | | D |
| 5 | **Department (e.g. HR, IT, etc.)** | **Name of IT System/ Software** | **If applicable: name and address of the Joint Controller** | **Categories of personal data** | **Purpose of processing** | **Categories of data subjects** | **Categories of recipients** including recipients in third countries or international organisations | **Transfer to third country or international organisation? (Name)** | **If applicable: Documentation of suitable safeguards for exceptional transfer to third country** (according to Art. 49 (1) sub. 2 GDPR?) | **Time limits for erasure for each category of data** | **General description of the technical and organisational security measures** | Wa |
| 6 | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | |
| 12 | | | | | | | | | | | | |

Record (as a controller) | Record (as a processor)

Ready | 90%

DE | 12:36 16.11.2016

# Posouzení vlivu na ochranu osobních údajů

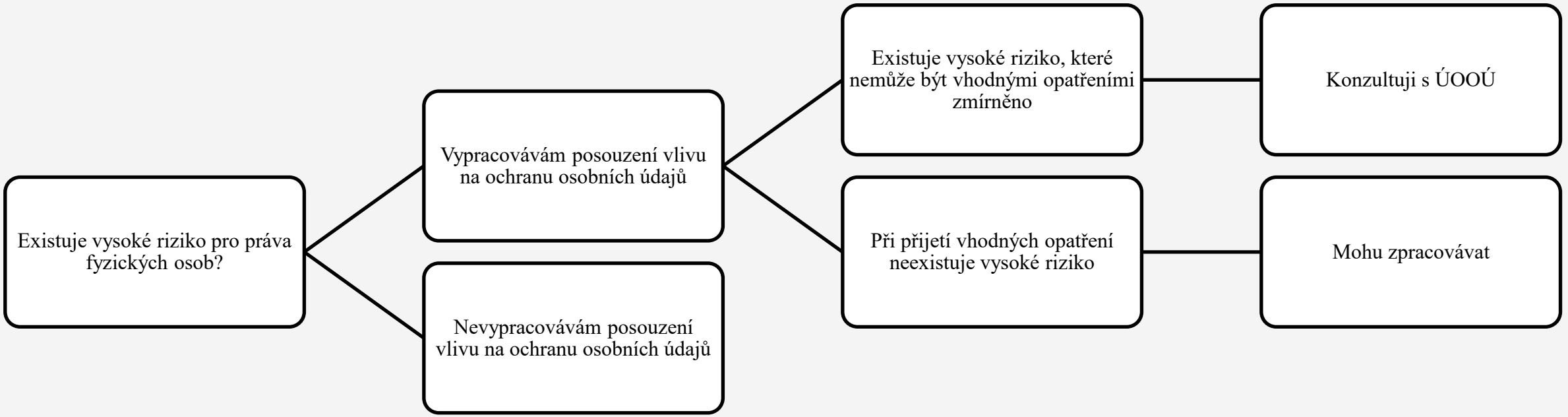
Vysoké riziko pro práva a svobody fyzických osob

- Monitorování veřejně přístupných prostor
- Rozsáhlé zpracování zvláštních kategorií oú
- Systematické vyhodnocování osobních aspektů

# Posouzení vlivu na ochranu osobních údajů

- Popis zamýšlených operací
- Posouzení nezbytnosti a přiměřenosti
- Posouzení rizik
- Opatření k řešení těchto rizik

# DPIA: předchozí konzultace



# Hlášení porušení

- Došlo k porušení zabezpečení?
- Dotýká se porušení osobních údajů?
- Jsou s tímto porušením spojeny rizika pro práva a svobody FO?
- Jsou tato rizika vysoká?

# Hlášení porušení ÚOOÚ

- Co se stalo
- Čeho se porušení dotklo
- Jméno a kontaktní údaje pověřence nebo jiného kontaktního místa
- Popis pravděpodobných důsledků

# 6. Pověřenec pro ochranu osobních údajů

# I. Kdo musí mít pověřence?

1. Orgán veřejné moci
2. Rozsáhlé a pravidelné monitorování
3. Rozsáhlé zpracování zvláštní kategorie údajů

# II. Co víme?

1. Velké nemocnice  - ANO
2. Jednotliví lékaři - NE

# III. Kdo může být pověřenec?

1. Znalost práva na ochranu osobních údajů
2. Znalost IT
3. Znalost interních procesů organizace

# IV. Co dělá pověřenec?

1. Poskytuje poradenství o zpracování
2. Monitoruje soulad s GDPR
3. Spolupracuje s ÚOOÚ
4. Kontaktní místo pro ÚOOÚ
5. Vyřizuje stížnosti

# 7. Shrnutí

# I. Zajištění souladu s GDPR:

1. Mapování
2. Vyhodnocení
3. Přijetí opatření

# II. Zajištění souladu s GDPR:

1. Právní opatření
2. Organizační opatření
3. Technická opatření

- **Vnitřní směrnice o ochraně osobních údajů**
- **Záznamy o činnostech zpracování**
- **Posouzení vlivu na ochranu osobních údajů**
- **Určení příslušnosti ve společnosti**

# Jak začít?

# 3 Vaše nejdůležitější kroky dnes:

# Jak Vám můžeme zjednodušit život?

holubova.cz

# Děkuji  za pozornost

**Štěpán Holub**

stepan.holub@holubova.cz