EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

LEGISLATIVA

Legislativa EU a ČR vztažená k ochraně osobních údajů – praktická aplikace

Metodický list

Autor: Ing. Jiří Sedláček, Metodik: Mgr. Hana Hrádková

Recenzent: Ing. Lukáš Přibyl

Rok vydání: 2023

Legislativa EU a ČR vztažená k ochraně osobních údajů – praktická aplikace podléhá licenci CC BY-SA 4.0 International License (Offline use: http://creative-commons.org/licenses/by-nc-sa/4.0/).

Obsah

1 Cíle 4
2 Dovednosti 4
3 Pracovní prostředí 5
4 Použitý model 5
5 Charakteristika cvičení 5
5.1 Hlavní zásady 5
5.2 Výhody 6
5.3 Nevýhody 6
6 Klíčové charakteristiky 6
7 Zainteresované strany 7
7.1 Soutěžící týmy 7
7.1.1 Očekávání od členů týmů 7
7.2 Moderátor, hodnotitel, pozorovatel 7
7.2.1 Moderátor 7
7.2.2 Hodnotitel 7
7.2.3 Pozorovatel 7
8 Průběh cvičení 8
8.1 Události 8
8.2 Odpovědi 8
8.3 Diskuze 8
8.4 Závěrečný debrief a vyhodnocení 8
9 Osnova výuky 9
Teoretická část 9
Praktická část 10
10 Input 1 – Věcná působnost GDPR, řešení problematiky OOÚ a určení OÚ a ZKOÚ 10
10.1 Věcná působnost GDPR 10

10.1.1 AK spolku doporučila skartovat kroniky spolku, případně umístěné fotografie z akcí spolku dodatečně „legalizovat“ získáním souhlasu se zpracováním OÚ od osob na fotografiích, v případě nezletilých osob získáním souhlasů od jejich zákonných zástupců. 10

10.2 Řešení problematiky OOÚ a určení OÚ a ZKOÚ 11

10.2.1 AK nabídla spolku své služby při vytvoření formuláře pro souhlas se zpracováním OÚ. Tyto souhlasy pak mají být zaměstnanci spolku (SÚ) podepsány a přiloženy k pracovním smlouvám. Souhlasy mají řešit zákonné zpracování OÚ zaměstnanců spolku obsažených v pracovních smlouvách. 11

10.2.2 Zdůvodněte, proč je právní základ „souhlas“ nestabilním? Pro svoje tvrzení uveďte důkaz. 11

10.2.3 V přiložené tabulce označte, u kterých informací se jedná z pohledu GDPR o OÚ (O) a u kterých informací se jedná o ZKOÚ (Z) 12

11 Input 2 – Pověřenec pro ochranu OÚ (DPO) 13

11.1 Uveďte na základě jakého ustanovení GDPR naše smyšlené zdravotnické zařízení jmenuje DPO. 13

11.2 O co lze opřít zákonné zpracování ZKOÚ zdravotnickým zařízením? 13

11.3 Uveďte z čeho vyplývá povinnost DPO být styčnou osobou pro komunikaci s ÚOOÚ 14

11.4 Postavení DPO v organizaci 14

11.4.1 Uveďte, jakým ustanovením je DPO umožněna jeho nezávislost a organizační začlenění v dané společnosti 14

11.4.2 Graficky znázorněte organizační začlenění DPO v organizaci 14

11.4.3 Jaké ustanovení GDPR zajistí DPO zdroje k plnění jeho úkolů a k udržování jeho odborné úrovně? 15

11.4.4 Jaké ustanovení GDPR určuje DPO, že je povinen chránit informace? 15

11.4.5 Jaké ustanovení GDPR umožňuje sdílení DPO? 15

12 Input 3 – Aplikace OOÚ 15

12.1 Správce a zpracovatel 15

12.1.1 Jakým způsobem se legalizuje zpracování OÚ zpracovatelem pro správce? Uveďte důkaz. 15

12.1.2 V jakém rozsahu a jakým způsobem musí vést správce záznamy o činnostech zpracování OÚ? Uveďte důkaz. 16

12.1.3 V jakém rozsahu a jakým způsobem musí vést zpracovatel záznamy o činnostech zpracování OÚ? Uveďte důkaz. 16

12.1.4 Kde je definována povinnost správce a zpracovatele poskytnout na vyžádání záznamy o zpracování OÚ ÚOOÚ? 16

12.2 Zpracování OÚ 17
12.2.1 Na jakou organizaci a za jakých podmínek se nevztahuje povinnost vést záznamy o činnostech zpracování OÚ? 17
12.2.2 Jaký článek GDPR požaduje zajištění ochrany informací – v tomto případě OÚ? 17
12.2.3 Co musí obsahovat hlášení o porušení zabezpečení OÚ dozorovému úřadu? 17
13 Input 4 – Práva SÚ 18
13.1 Jaké články řeší práva SÚ? Uveďte jejich výčet. 18
13.1.1 Jaký ze článků uvedených v předchozím dotazu řeší právo SÚ nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování? 19
13.2 Jaký zákon ČR ve veřejném zájmu popírá právo SÚ na výmaz? Jedná se např. o případ, kdy občan vyžaduje po střední škole vystavení opisu maturitního vysvědčení… Uveďte důkaz z GDPR a číslo a název příslušnoho zákona. 19
13.3 U přiloženého obrázku uveďte zda-li byla porušena práva SÚ a pokud ano, uveďte zdůvodnění z GDPR… 20
13.4 U přiloženého obrázku uveďte zda-li byla porušena práva SÚ a pokud ano, uveďte zdůvodnění z GDPR… 21
Shrnutí a závěr 22
Seznam použité literatury 23
Odkazy na použité zákonné předpisy 24

1 Cíle

Uvedení všech cílů, kterých bude v rámci této úlohy dosaženo, dle Bloomovy taxonomie výukových cílů (viz. Příloha 1)

- Porozumět smyslu práva v rámci fungování státu.
- Pochopit hierarchii právních norem podle právní síly a vliv právních předpisů EU na právní předpisy ČR.
- Pochopit dopady legislativy EU na ochranu osobních údajů v ČR.
- Pochopit smysl a strukturu GDPR[1] a zákona č. 110/2019 Sb.[2]
- Pochopit roli ÚOOÚ[3] coby ústředního správního orgánu v oblasti ochrany osobních údajů.
- Pochopit pravidla pro zavedení ochrany osobních údajů v organizaci a jejich praktickou aplikaci.
- Aplikovat principy ochrany osobních údajů do vnitřních předpisů právnické osoby.

- Naučit se pracovat s textací GDPR.
- Naučit se pracovat s webem ÚOOÚ.
- Porozumět významu a smyslu ochrany osobních údajů a osvojit si praktickou aplikaci.
- Prohloubit znalosti účastníků cvičení v oblasti ochrany osobních údajů.
- Umožnit účastníkům cvičení sdílení zkušeností a názorů, včetně tréninku týmové práce a spolupráce.
- Rozvoj analytického myšlení. Uvažování v souvislostech.

2 Dovednosti

- Pracovat se zákonnými předpisy relevantními k cvičenému tématu.
- Aplikovat legislativu ČR dle hierarchie právních hodnot podle právní síly do vnitřních předpisů organizace.
- Aplikovat konkrétní ustanovení GDPR do vnitřních předpisů organizace.
- Pracovat s webem ÚOOÚ.
- Vyjednávat v týmu o řešeních stanovené problematiky.
- Sdílet v týmech názory, znalosti a stanoviska.

[1] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
[2] Zákon č. 110/2019 Sb., o zpracování osobních údajů
[3] Úřad pro ochranu osobních údajů – www.uoou.cz

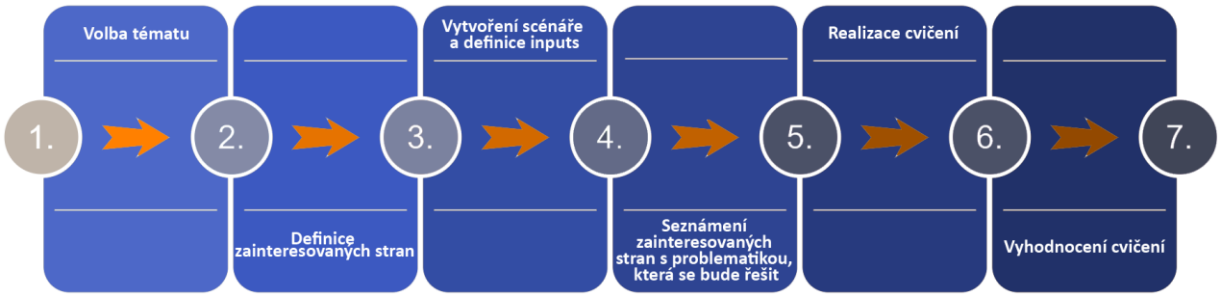
3 Pracovní prostředí

- Úlohu lze realizovat v učebně vybavené výpočetní technikou, tabulí s popisovači, projektorem a místem pro jednotlivé týmy.

Pro práci jsou vhodné následující pomůcky:

- Psací potřeby.
- Poznámkové bloky.
- Dle potřeb popisovací lepíky.
- Projektor s promítacím prostorem (plátno/stěna).
- Počítač s rozhraním pro připojení projektoru.

4 Použitý model



5 Charakteristika cvičení

Tabletop cvičení je druh tréninku, při němž je možné celkem nenákladnou formou procvičit navozená témata, včetně organizačních a technických opatření a znalostí k tomu potřebných. Cvičení je realizováno účastí jednotlivých týmů tzv. „u stolu“.

5.1 Hlavní zásady

- Týmový duch.
- Soutěživost.
- Spolupráce.
- Sdílení znalostí.
- Brainstorming.
- Rovnost názorů.

5.2 Výhody

- Nízko stresové prostředí.
- Nízké náklady.
- Průběžné hodnocení.
- Moderovaná skupinová diskuse o problémových oblastech.

5.3 Nevýhody

- Chybí reálný prožitek.
- Nejedná se o skutečný test provozní schopnosti.
- V rámci simulace je poskytnut pouze povrchní pohled na danou organizaci.

6 Klíčové charakteristiky

- Tento typ cvičení slouží k seznámení zúčastněných osob se související tématikou a k řešení navozené situace či témat. Cílem není hodnotit správnost odpovědí.
- V rámci týmu jsou určeny role a to tak, aby bylo cvičení co nejpřínosnější.
- Navozená situace či řešená témata vyžadují efektivní týmové rozhodování, a to navzdory nedostatku informací a časovému tlaku.
- Přínosnou a žádanou je diskuze, a to jak v týmech, tak i mezi týmy. Vede nejen k učinění relevantního rozhodnutí, ale je i přínosem cvičení.
- Každému rozhodnutí je vhodné předřadit relevantní faktory/roviny (bezpečnostní, věcné, právní, politické, ekonomické, mediální…).
- Navozená situace nemusí být vždy smyšlená. Může být inspirována skutečnou událostí.
- Scénář může popisovat děj podobný ději v reálném světě, v ČR, ve smyšlené organizaci.
- Je žádoucí řešit vždy pouze navozenou situaci či témata.

7 Zainteresované strany

7.1 Soutěžící týmy

- Cvičení se zúčastní 4 týmy po 5 členech.
- V tomto konkrétním cvičení se nerozlišují role jednotlivých aktérů s výjimkou určení zástupce za každý tým pro komunikaci jménem týmu.
- Týmy mají k dispozici tento manuál a další materiály potřebné k účasti na cvičení – viz níže.

7.1.1 Očekávání od členů týmů

Nezdráhejte se zapojit do konverzace. Buďte aktivní, vyzývejte i ostatní členy týmu k zapojení do diskuze. Je v pořádku nemít odpověď. Přijměte představený scénář a pracujte v rámci uvedených parametrů.

7.2 Moderátor, hodnotitel, pozorovatel

7.2.1 Moderátor

- Zástupce školy, případně externí spolupracovník.
- Moderátor má k dispozici tento manuál a materiály s klíčem k řešení událostí a inputs.

7.2.1.1 Činnosti moderátora

- Seznámí týmy se scénářem/tématy.
- Řídí čas.
- Operativně reaguje v rámci nastalé situace atd.
- Kontrolujte tempo a průběh cvičení.
- Stimulujte a řídí diskusi.
- V případě potřeby dodává vodítka.
- Získává odpovědi a řešení od týmů.

7.2.2 Hodnotitel

- Zástupce školy, případně externí spolupracovník.
- Hodnotitel je seznámen s navozeným tématem či situací v rámci daného cvičení.

7.2.2.1 Činnosti hodnotitele

- U Týmů identifikujte silné stránky a oblasti zlepšení.
- Pomáhá vypracovat zprávu po cvičení.

7.2.3 Pozorovatel

- Zástupce školy, případně externí spolupracovník.
- Pozorovatel je seznámen s navozeným tématem či situací v rámci daného cvičení.

7.2.3.1 Činnosti pozorovatele

- Účastní se diskuze, pokud je požádán.

Pozn.: Pro potřeby cvičení, v prostředí organizace typu střední škola, je možné, s cílem snížení nároků na personální zdroje, role moderátora, hodnotitele a pozorovatele sloučit do jedné role.

8 Průběh cvičení

8.1 Události

- Scénář cvičení je koncipován tak, že dané téma je řešeno v několika oddělených vstupech (inputs – viz materiál pro týmy). Ta budou vždy moderátorem představena ať už ústně či za pomoci prezentace.
- V rámci každého inputu obdrží každý tým otázky, případně formulář pro zaznamenání odpovědí. Otázky mohou být doplněny i grafickými informacemi. Vše je nutné pečlivě přečíst a zanalyzovat.
- Na analýzu každé navozené situace v rámci inputu je určen časový limit, který moderátor hlídá.
- V některých případech, kdy k tomu dá moderátor svolení, bude možné použít internetu jako zdroje informací.

8.2 Odpovědi

- Na každou položenou otázku odpovězte ve stanoveném čase.
- Protože se jedná o týmovou práci, otázky v týmu diskutujte a odpovědi formulujte jako tým společně.
- V případě, že se nemůžete v rámci týmu na výsledné odpovědi shodnout, zaznamenejte to do odpovědního formuláře.

8.3 Diskuze

- Mimo diskuze v týmech je možná taktéž diskuze mezi týmy.
- Tuto diskuzi iniciuje a řídí výhradně pouze moderátor (a to i neplánovaně podle průběhu cvičení).

8.4 Závěrečný debrief a vyhodnocení

- Po uplynutí stanoveného programu a času bude cvičení ukončeno.
- Moderátor ve spolupráci s hodnotitelem cvičení vyhodnotí.

V dohodnutém termínu bude cvičení za přítomnosti všech týmů shrnuto a účastníci budou seznámeni s výsledky.

9 Osnova výuky

Výuka je rozdělena na teoretickou a praktickou část.

Teoretická část

Před realizací cvičení (Praktická část) je nezbytné ujistit se, že témata řešená v Praktické části jsou pro studenty známá, pochopená a srozumitelná.

Pokud jsou v praktické části identifikovány oblasti, které nejsou součástí standardního vzdělávání, je nutné je před realizací cvičení se studenty probrat. Pro účely seznámení je možné použít právě témata cvičená v jednotlivých Inputs praktické části této metodiky (v metodice jsou vždy uvedeny správné odpovědi a řešení).

Jako informačního zdroje je možné použít zákonné normy/oblasti, které jsou uvedeny v Použité literatuře, v kontextu k řešeným úkolům v rámci Praktické části.

Praktická část

10 Input 1 – Věcná působnost GDPR, řešení problematiky OOÚ[4] a určení OÚ[5] a ZKOÚ[6]

10.1 Věcná působnost GDPR

Předmětem tohoto Inputu je dětský spolek Zajíci.

Název spolku: **Zajíci** Právní forma: **příspěvková organizace** Účel: **tělovýchovná, sportovní, kulturní, vlastivědná a společenská činnost** Spolek po nabytí účinnosti GDPR kontaktovala advokátní kancelář (dále jen AK) s nabídkou placené pomoci řešení problematiky OOÚ ve spolku.

10.1.1 AK spolku doporučila skartovat kroniky spolku, případně umístěné fotografie z akcí spolku dodatečně „legalizovat“ získáním souhlasu se zpracováním OÚ od osob na fotografiích, v případě nezletilých osob získáním souhlasů od jejich zákonných zástupců.

Potvrďte relevanci tohoto požadavku a uveďte pro svoje tvrzení důkaz.

Čas na zpracování odpovědi: 15‘

Požadavek AK je irelevantním.
Odůvodnění: GDPR, Článek 2, odstavec 1)
Toto nařízení se vztahuje na **zcela** nebo **částečně automatizované** zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v **evidenci** nebo do ní mají být zařazeny.
U fotografií v kronikách umístěných se nejedná ani o zcela či částečně automatizované zpracování OÚ, či o jejich obsažení v „evidenci“.
Pozn. Pro Moderátora: věcná působnost GDPR a popis významu „evidence“ jsou cvičeny v OOU Prac_L01.

[4] OOÚ – ochrana osobních údajů
[5] OÚ – osobní údaj
[6] ZKOÚ – zvláštní kategorie osobních údajů

10.2 Řešení problematiky OOÚ a určení OÚ a ZKOÚ

10.2.1 AK nabídla spolku své služby při vytvoření formuláře pro souhlas se zpracováním OÚ. Tyto souhlasy pak mají být zaměstnanci spolku (SÚ[7]) podepsány a přiloženy k pracovním smlouvám. Souhlasy mají řešit zákonné zpracování OÚ zaměstnanců spolku obsažených v pracovních smlouvách.

Potvrďte relevanci tohoto požadavku a uveďte pro svoje tvrzení důkaz.

Čas na zpracování odpovědi: 15'

Požadavek AK je irelevantním.

Odůvodnění:
GDPR, Článek 6, Zákonnost zpracování, b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo za účelem přijetí opatření na žádost subjektu údajů před uzavřením smlouvy;
Z výše uvedeného je zřejmé, že právní základ typu „souhlas" je zde nadbytečným a zavádějícím. Zákonnost zpracování je viz výše v souladu s GDPR.

10.2.2 Zdůvodněte, proč je právní základ „souhlas" nestabilním? Pro svoje tvrzení uveďte důkaz.

Čas na zpracování odpovědi: 15'

Právní základ právní základ „souhlas" je nestabilním pro jeho závislost na svobodné vůli SÚ. Nestabilita souhlasu spočívá v právu SÚ jej kdykoli svobodně odvolat – viz zdůvodnění níže.

Odůvodnění:
GDPR
Článek 7
Podmínky vyjádření souhlasu
3. Subjekt údajů má **právo svůj souhlas kdykoli odvolat**. Odvoláním souhlasu není dotčena zákonnost zpracování založeného na souhlasu před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně snadné jako jej poskytnout.

Článek 17
Právo na výmaz („právo být zapomenut")
1. Subjekt údajů má **právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají**, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:
b) subjekt údajů odvolá souhlas, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) zpracovány, a neexistuje žádný další právní důvod pro zpracování;

[7] SÚ – subjekt údajů

10.2.3 V přiložené tabulce označte, u kterých informací se jedná z pohledu GDPR o OÚ (O) a u kterých informací se jedná o ZKOÚ (Z)

Čas na zpracování odpovědi: 15‘

Určení OÚ a ZKOÚ		
Příklady	**OÚ**	**ZKOÚ**
jméno a příjmení	O	
adresa (ulice, číslo popisné, směrovací číslo, město) ve spojení např. s pohlavím a věkem	O	
jméno		
e-mailová adresa ve formátu jméno.příjmení@firma.com	O	
barva vlasů ve spojení např. s pohlavím a věkem a bydlištěm	O	
rodné číslo	O	
barva vlasů		
adresa IP (Internetový protokol) v uvedené firmě	O	
telefonní číslo	O	
IČ	O	
DIČ	O	
číslo OP	O	
číslo ŘP	O	
číslo cestovního pasu	O	
otisk prstu		Z
biometrické informace		Z
snímek oční duhovky		Z
snímek sítnice		Z
podpis		Z
výška		
výška v kombinaci s věkem, pohlavím a bydlištěm		

11 Input 2 – Pověřenec pro ochranu OÚ (DPO[8])

Předmětem tohoto Inputu je smyšlené zdravotnické zařízení Zemská nemocnice Priessnitz

Nemocnice poskytuje zdravotní služby v souladu se zákonem č. 372/2011 Sb., zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách).

11.1 Uveďte na základě jakého ustanovení GDPR naše smyšlené zdravotnické zařízení jmenuje DPO.

Čas na zpracování odpovědi: 15‘

Oddíl 4
Pověřenec pro ochranu osobních údajů
Článek 37
Jmenování pověřence pro ochranu osobních údajů
Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy:
c) hlavní činnosti správce nebo zpracovatele spočívají v **rozsáhlém zpracování zvláštních kategorií údajů** uvedených v článku 9 nebo osobních údajů týkajících se odsouzení v trestních věcech a trestných činů uvedených v článku 10.

11.2 O co lze opřít zákonné zpracování ZKOÚ zdravotnickým zařízením?

Čas na zpracování odpovědi: 15‘

KAPITOLA II
Zásady
Článek 9, Zpracování zvláštních kategorií osobních údajů
Odstavec 2
h) **zpracování je nezbytné pro účely preventivního nebo pracovního lékařství**, pro posouzení pracovní schopnosti zaměstnance, **lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb**

[8] DPO – Data Protection Officer – Pověřenec pro ochranu osobních údajů

zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v odstavci 3.

11.3 Uveďte z čeho vyplývá povinnost DPO být styčnou osobou pro komunikaci s ÚOOÚ[9]

Čas na zpracování odpovědi: 10‘

Článek 39
Úkoly pověřence pro ochranu osobních údajů
1. Pověřenec pro ochranu osobních údajů vykonává alespoň tyto úkoly:
e) působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36, a případně vedení konzultací v jakékoli jiné věci.

11.4 Postavení DPO v organizaci

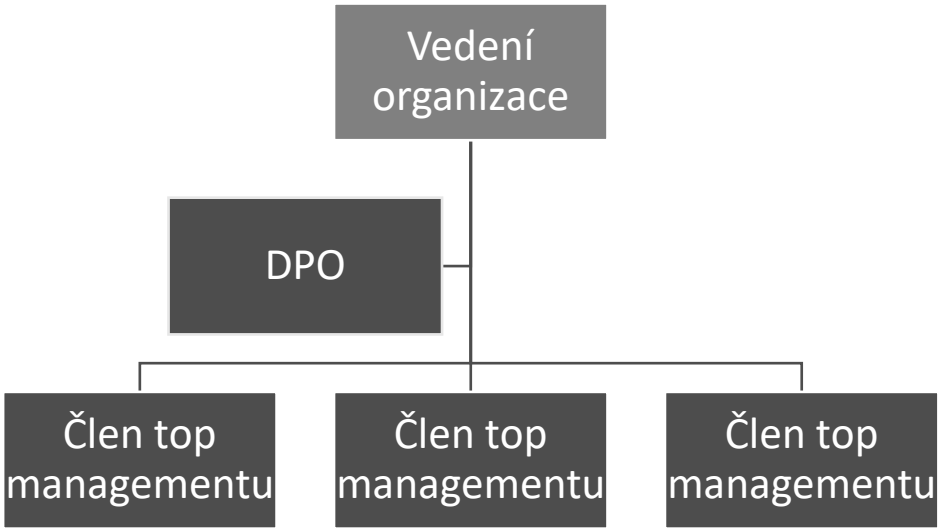
11.4.1 Uveďte, jakým ustanovením je DPO umožněna jeho nezávislost a organizační začlenění v dané společnosti

Čas na zpracování odpovědi: 10‘

Oddíl 4
Pověřenec pro ochranu osobních údajů
Článek 38
Postavení pověřence pro ochranu osobních údajů
3. Správce a zpracovatel zajistí, aby pověřenec pro ochranu osobních údajů 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.

11.4.2 Graficky znázorněte organizační začlenění DPO v organizaci

Čas na zpracování odpovědi: 10‘



[9] ÚOOÚ – ústřední správní orgán pro oblast ochrany osobních údajů – Úřad pro ochranu osobních údajů

11.4.3 Jaké ustanovení GDPR zajistí DPO zdroje k plnění jeho úkolů a k udržování jeho odborné úrovně?

Čas na zpracování odpovědi: 10‘

Oddíl 4
Pověřenec pro ochranu osobních údajů
Článek 38
Postavení pověřence pro ochranu osobních údajů
2. Správce a zpracovatel podporují pověřence pro ochranu osobních údajů při plnění úkolů uvedených v článku 39 tím, že mu poskytují zdroje nezbytné k plnění těchto úkolů, přístup k osobním údajům a operacím zpracování a zdroje nezbytné k udržování jeho odborných znalostí.

11.4.4 Jaké ustanovení GDPR určuje DPO, že je povinen chránit informace?

Čas na zpracování odpovědi: 10‘

Oddíl 4
Pověřenec pro ochranu osobních údajů
Článek 38
Postavení pověřence pro ochranu osobních údajů
5. Pověřenec pro ochranu osobních údajů je v souvislosti s výkonem svých úkolů vázán tajemstvím nebo důvěrností, v souladu s právem Unie nebo členského státu.

11.4.5 Jaké ustanovení GDPR umožňuje sdílení DPO?

Čas na zpracování odpovědi: 10‘

Oddíl 4
Pověřenec pro ochranu osobních údajů
Článek 37
Jmenování pověřence pro ochranu osobních údajů
2. Skupina podniků může jmenovat jediného pověřence pro ochranu osobních údajů, pokud je snadno dosažitelný z každého podniku.

12 Input 3 – Aplikace OOÚ

12.1 Správce a zpracovatel

12.1.1 Jakým způsobem se legalizuje zpracování OÚ zpracovatelem pro správce? Uveďte důkaz.

Čas na zpracování odpovědi: 10‘

Zpracovatel smí OÚ zpracovávat pro správce na základě uzavřené zpracovatelské smlouvy.

Článek 28
Zpracovatel
3. Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce.

12.1.2 V jakém rozsahu a jakým způsobem musí vést správce záznamy o činnostech zpracování OÚ? Uveďte důkaz.

Čas na zpracování odpovědi: 15‘

Článek 30
Záznamy o činnostech zpracování
1. Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá. Tyto záznamy obsahují všechny tyto informace:
a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;
b) účely zpracování;
c) popis kategorií subjektů údajů a kategorií osobních údajů;
d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;
f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;
g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.

3. Záznamy podle odstavců 1 a 2 se vyhotovují písemně, v to počítaje i elektronickou formu.

12.1.3 V jakém rozsahu a jakým způsobem musí vést zpracovatel záznamy o činnostech zpracování OÚ? Uveďte důkaz.

Čas na zpracování odpovědi: 15‘

Článek 30
Záznamy o činnostech zpracování
2. Každý zpracovatel a jeho případný zástupce vede záznamy o všech kategoriích činností zpracování prováděných pro správce, jež obsahují:
a) jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů;
b) kategorie zpracování prováděného pro každého ze správců;
c) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;
d) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.

3. Záznamy podle odstavců 1 a 2 se vyhotovují písemně, v to počítaje i elektronickou formu.

12.1.4 Kde je definována povinnost správce a zpracovatele poskytnout na vyžádání záznamy o zpracování OÚ ÚOOÚ?

Čas na zpracování odpovědi: 10‘

Článek 30
Záznamy o činnostech zpracování
4. Správce, zpracovatel nebo případný zástupce správce nebo zpracovatele poskytne záznamy na požádání dozorového úřadu.

12.2 Zpracování OÚ

12.2.1 Na jakou organizaci a za jakých podmínek se nevztahuje povinnost vést záznamy o činnostech zpracování OÚ?

Čas na zpracování odpovědi: 10‘

Článek 30
Záznamy o činnostech zpracování
5. Povinnosti uvedené v odstavcích 1 a 2 se nepoužijí pro podnik nebo organizaci zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se odsouzení v trestních věcech a trestných činů uvedených v článku 10.

12.2.2 Jaký článek GDPR požaduje zajištění ochrany informací – v tomto případě OÚ?

Čas na zpracování odpovědi: 10‘

Oddíl 2
Zabezpečení osobních údajů
Článek 32
Zabezpečení zpracování

12.2.2.1 Ve kterém písmenu je požadováno zajištění kontinuity byznysu?

Čas na zpracování odpovědi: 15‘

Oddíl 2
Zabezpečení osobních údajů
Článek 32
Zabezpečení zpracování
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

12.2.2.2 V jakém písmenu je požadováno zajištění testování zavedených bezpečnostních opatření?

Čas na zpracování odpovědi: 15‘

d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění zabezpečení zpracování.

12.2.3 Co musí obsahovat hlášení o porušení zabezpečení OÚ dozorovému úřadu?

Čas na zpracování odpovědi: 15‘
Článek 33
Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu
3. Ohlášení podle odstavce 1 musí přinejmenším obsahovat:
a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;
c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

12.2.3.1 Jaká je lhůta pro nahlášení případů porušení zabezpečení osobních údajů dozorovému úřadu?

Čas na zpracování odpovědi: 15‘

Článek 33
Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu
Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

12.2.3.2 V jakém případě se musí nahlásit porušení zabezpečení osobních údajů SÚ?

Čas na zpracování odpovědi: 10‘

Článek 34
Oznamování případů porušení zabezpečení osobních údajů subjektu údajů
Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů.

Tady taky řešit přednostní právo zákona o archivnictví a spisové službě

Weby eshopů – nesvobodný souhlas

13 Input 4 – Práva SÚ

13.1 Jaké články řeší práva SÚ? Uveďte jejich výčet.

Čas na zpracování odpovědi: 10‘

Článek 15
Právo subjektu údajů na přístup

Článek 16
Právo na opravu

Článek 17
Právo na výmaz („právo být zapomenut“)

Článek 18
Právo na omezení zpracování

Článek 19

Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

Článek 20
Právo na přenositelnost údajů

Článek 21
Právo vznést námitku

Článek 22
Automatizované individuální rozhodování, včetně profilování

13.1.1 Jaký ze článků uvedených v předchozím dotazu řeší právo SÚ nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování?

Čas na zpracování odpovědi: 5‘

Článek 22
Automatizované individuální rozhodování, včetně profilování

13.2 Jaký zákon ČR ve veřejném zájmu popírá právo SÚ na výmaz? Jedná se např. o případ, kdy občan vyžaduje po střední škole vystavení opisu maturitního vysvědčení… Uveďte důkaz z GDPR a číslo a název příslušnoho zákona.

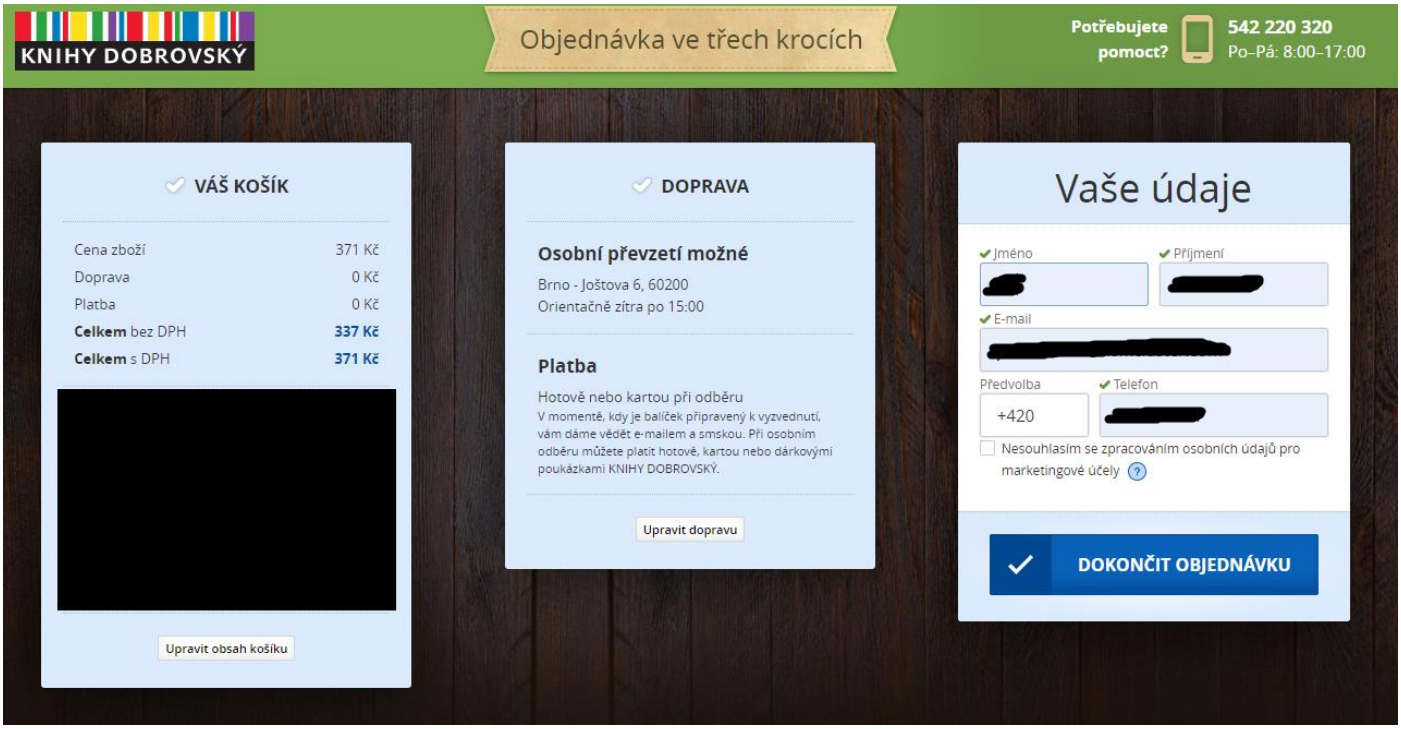
Čas na zpracování odpovědi: 5‘

Článek 17
Právo na výmaz („právo být zapomenut“)
3. Odstavce 1 a 2 se neuplatní, pokud je zpracování nezbytné:
d) **pro účely archivace ve veřejném zájmu**, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1, pokud je pravděpodobné, že by právo uvedené v odstavci 1 znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování;

Jedná se o zákon č. 499/2004 Sb. o archivnictví a spisové službě.

13.3 U přiloženého obrázku uveďte zda-li byla porušena práva SÚ a pokud ano, uveďte zdůvodnění z GDPR.

Čas na zpracování odpovědi: 15‘



Tento souhlas není v pořádku, protože je defaultně nastaven checkbox tak, že zákazník vyjadřuje souhlas se zpracováním OÚ. Zpracovatel se v tomto případě spoléhá na nepozornost zákazníka.

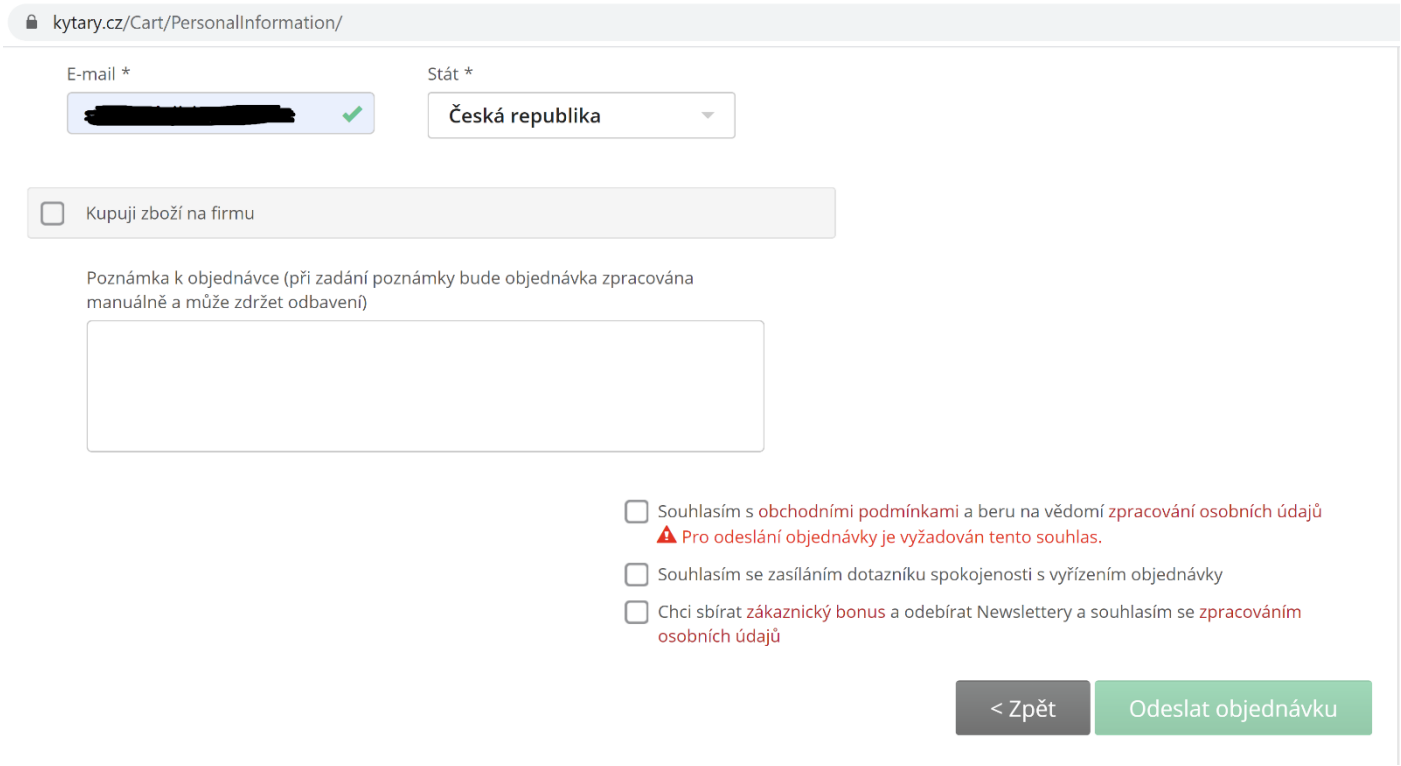
Důkaz:

(32) Souhlas by měl být dán jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů, které se jej týkají, a to v podobě písemného prohlášení, i učiněného elektronicky, nebo ústního prohlášení. Mohlo by se například jednat o zaškrtnutí políčka při návštěvě internetové stránky, volbu technického nastavení pro služby informační společnosti nebo jiné prohlášení či jednání, které v této souvislosti jasně signalizuje souhlas subjektu údajů s navrhovaným zpracováním jeho osobních údajů. Mlčení, předem zaškrtnutá políčka nebo nečinnost by tudíž neměly být považovány za souhlas. Souhlas by se měl vztahovat na veškeré činnosti zpracování prováděné pro stejný účel nebo stejné účely. Jestliže má zpracování několik účelů, měl by být souhlas udělen pro všechny. Má-li subjekt údajů vyjádřit souhlas na základě žádosti podané elektronickými prostředky, musí být žádost jasná a stručná a nesmí zbytečně narušit využívání služby, pro kterou je souhlas dáván.

Článek 4
Definice
Pro účely tohoto nařízení se rozumí:
„souhlasem“ subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

13.4 U přiloženého obrázku uveďte zda-li byla porušena práva SÚ a pokud ano, uveďte zdůvodnění z GDPR.

Čas na zpracování odpovědi: 15‘



Tento souhlas je nesvobodným, protože je zákazník nucen jej udělit. V opačném případě není schopen dokončit objednávku zboží. Často se děje tento neduh, kdy je souhlas svázán s obchodními podmínkami. Navíc často používaná formulace „beru na vědomí zpracování osobních údajů“ je zavádějící. Na první pohled není zřejmé jestli se jedná o souhlas, či o něco jiného…

Důkaz:

(42) Pokud je zpracování založeno na souhlasu subjektu údajů, měl by být správce schopen prokázat, že subjekt údajů vyjádřil s danou operací zpracování souhlas. Zejména v případě písemného prohlášení souvisejícího s jinou skutečností by mělo být pomocí záruk zajištěno, že si je subjekt údajů vědom toho, že dává souhlas a v jakém rozsahu. V souladu se směrnicí Rady 93/13/EHS(10) by prohlášení o souhlasu navržené správcem mělo být poskytnuto ve srozumitelném a snadno přístupném znění za použití jasného a jednoduchého jazyka a nemělo by obsahovat nepřiměřené podmínky. Aby se zajistilo, že souhlas bude informovaný, měl by subjekt údajů znát alespoň totožnost správce a účely zpracování, k nimž jsou jeho osobní údaje určeny. **Souhlas by neměl být považován za svobodný, pokud subjekt údajů nemá skutečnou nebo svobodnou volbu** nebo nemůže souhlas odmítnout nebo odvolat, aniž by byl poškozen.

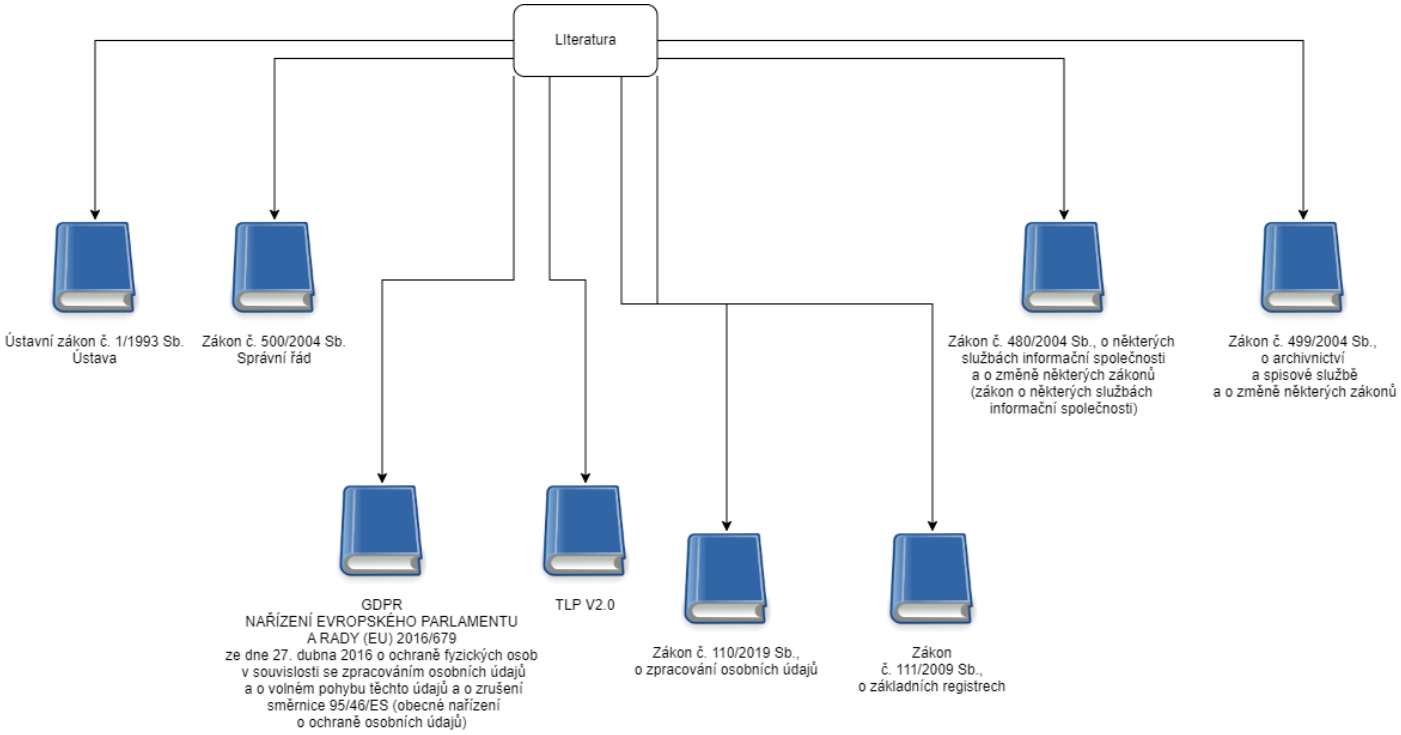
Článek 4
Definice
Pro účely tohoto nařízení se rozumí:
„souhlasem“ subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

Shrnutí a závěr

Po absolvování tohoto cvičení budou studenti schopni:

- Pochopit způsoby aplikace práva EU do legislativy ČR.
- Pochopit smysl aplikace práva pro oblast ochrany osobních údajů.
- Pochopit praktickou aplikaci OOÚ v organizaci.
- Prakticky ověřit, že pro každou právnickou osobu je nezbytné zajistit v rámci své činnosti ochranu zpracovávaných osobních údajů v souladu s relevantními zákonnými předpisy.

Seznam použité literatury



Odkazy na použité zákonné předpisy

Zákonné předpisy

- Zákony pro lidi
  https://www.zakonyprolidi.cz
- Ústava ČR - ústavní zákon č. 1/1993 Sb.
  https://www.zakonyprolidi.cz/cs/1993-1
- Zákon č. 372/2011 Sb., zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)
  https://www.zakonyprolidi.cz/cs/2011-372
- Zákon č. 500/2004 Sb., správní řád
  https://www.zakonyprolidi.cz/cs/2004-500
- Zákon o zpracování osobních údajů
  https://www.zakonyprolidi.cz/cs/2019-110?text=110%2F2019
- Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)
  https://www.zakonyprolidi.cz/cs/2004-480?text=z%C3%A1kon+o+n%C4%9Bkter%C3%BDch+slu%C5%BEb%C3%A1ch+in-forma%C4%8Dn%C3%AD+spole%C4%8Dnosti
- Zákon č. 499/2004 Sb. o archivnictví a spisové službě
  https://www.zakonyprolidi.cz/cs/2004-499
- Zákon č. 111/2009 Sb., o základních registrech
  https://www.zakonyprolidi.cz/cs/2009-111?text=z%C3%A1kon+o+z%C3%A1kladn%C3%ADch+registrech

Úřad - web ÚOOÚ
GDPR
https://www.uoou.cz/obecne%2Dnarizeni%2Do%2Dochrane%2Dosobnich%2Dudaju%2Dgdpr/ds-3938/p1=3938

Web MVCR
https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx

TLP
https://www.nukib.cz/cs/infoservis/doporuceni/1862-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci-2/

Podpůrné materiály:

- Výkladový slovník kybernetické bezpečnosti
  https://www.nukib.cz/download/publikace/podpurne_materialy/vykladovy_slovnik_KB_3_vydani.pdf

Použitá literatura:

ČADOVÁ, Barbara, Jana PETRŽELOVÁ a Miroslava ČERMÁKOVÁ. *Maturitní otázky -občanský a společenskovědní základ*. 1. vyd. Fragment, 2008, 224 s. ISBN 978-80-253-0600-0.

Důvěrnost informací v souladu s TLP 2.0

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta.
TLP:AMBER+STRICT	Informace je sdílena pouze s organizací.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Příklady použití:

TLP:RED – Od zahraničních partnerů jsme získali informaci, že útočník má přístup do vaší sítě a plánuje spustit ransomware útok. Doporučujeme tedy provést následující protiopatření...

TLP:AMBER – Z našich zjištění vyplývá, že je ve vaší síti používána zranitelná verze firewallu. Doporučujeme co nejdříve provést jeho aktualizaci. Tuto informaci můžete předat správci nebo dodavateli FW.

TLP:AMBER+STRICT – Z našich zjištění vyplývá, že je ve vaší síti používána zranitelná verze firewallu. Doporučujeme co nejdříve provést jeho aktualizaci. Tuto informaci je možné předat pouze v rozsahu vaší organizace.

TLP:GREEN – V České republice nyní probíhá phishing kampaň zaměřující se na zdravotnická zařízení, poučte své uživatele na možná rizika.

TLP:CLEAR – GovCERT.CZ za poslední rok řešil 126 incidentů, z toho 26 závažných.

Pro vice informací o protokolu sledujte oficiální stránky FIRST: https://www.first.org/tlp/