Príloha č. 1

Opis predmetu zákazky

Predmet zákazky:

Analýza stavu spracovania osobných údajov vzhľadom na požiadavky vyplývajúce z Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR)

Podrobný opis predmetu zákazky

1. Vstupná analýza súčasného stavu ochrany osobných údajov vykonaná formou konzultácií, vyplnením dotazníka a osobnou obhliadkou s cieľom identifikovať a vyhodnotiť:
- rozsah a potrebnosť spracúvania osobných údajov,
- právne základy spracúvania osobných údajov (legislatíva, súhlas),
- plnenie informačnej povinnosti,
- toky údajov v rámci organizácie,
- zmluvné vzťahy so sprostredkovateľmi,
- zmluvné vzťahy s poskytovateľmi služieb, najmä IKT, ktorí nie sú spracovateľmi v zmysle zákona,
- úroveň prijatých bezpečnostných opatrení pri spracúvaní osobných údajov (technické, organizačné),
- rozsah spracovanej bezpečnostnej dokumentácie k ochrane osobných údajov,
- úroveň a rozsah kontrolnej činnosti.

2. GAP/rozdielová analýza:
- analýza rozdielov v súčasnosti platných opatrení v podmienkach organizácie voči požiadavkám vyplývajúcich z GDPR. V prípadoch identifikácie nesúladu alebo čiastočného nesúladu s požiadavkami GDPR návrh odporúčaní na ich odstránenie.

3. Aktualizácia analýzy rizík vykonanej v súlade so zákonom č. 122/2013 Z. z. o ochrane osobných údajov, ktorá pozostáva z nasledujúcich krokov:
- identifikácia a ohodnotenie aktív,
- identifikácia a ohodnotenie hrozieb pre aktíva,
- identifikácia a ohodnotenie miest zraniteľností, ktoré môžu byť využité na realizáciu hrozby,
- identifikácia a ohodnotenie možných dopadov pre organizáciu v dôsledku narušenia dôvernosti, integrity alebo dostupnosti aktív,
- určenie miery rizika,
- identifikácia realizovaných bezpečnostných opatrení a určenie miery rizika po zvážení účinnosti realizovaných opatrení,
- návrh ďalších opatrení na zníženie miery rizika/zvýšenie úrovne bezpečnosti prostredia.

4. Aktualizácia a dopracovanie dokumentácie v rozsahu:
- aktualizácia bezpečnostnej dokumentácie,
- vypracovanie interných politík aj dokumentov na plnenie info povinností voči dotknutým osobám
- „Posúdenie vplyvu na ochranu údajov"/DPIA, ktoré bude obsahovať systematický opis plánovaných spracovateľských operácii a účely spracúvania; posúdenie nutnosti a primeranosti spracovateľských operácii vo vzťahu k účelu; posúdenie rizika pre práva a slobody dotknutých osôb; opatrenia na riešenie rizík, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s nariadením; zohľadnenie práv a oprávnených záujmov dotknutých osôb a ďalších osôb, ktorých sa zamýšľané spracúvanie týka.

5. Realizácia zmien vyplývajúcich z pripravovaného zákona o ochrane osobných údajov
- zapracovanie prípadných zmien do bezpečnostnej dokumentácie.

6. Úprava sprostredkovateľských vzťahov v zmysle požiadaviek GDPR a pripravovaného zákona v rozsahu:
- úprava sprostredkovateľských vzťahov zameraná na zosúladenie zmlúv s požiadavkami GDPR a pripravovaného zákona a návrh nových opatrení na zabezpečenie primeranej úrovne ochrany osobných údajov.

7. Preškolenie zamestnancov v zmysle požiadaviek GDPR a pripravovaného zákona:
- preškolenie zamestnancov (napr. skupinové školenie určené pre oprávnené osoby , prípadne formou e-learningu).

ÚVODNÝ DOTAZNÍK
ZA ÚČELOM ZABEZPEČENIA SÚLADU S GDPR
V PODMIENKACH
OPERAČNÉHO STREDISKA

General Data Protection Regulation („GDPR" alebo „Nariadenie") predstavuje najväčšiu zmenu v oblasti ochrany súkromia za posledných 20 rokov. Bude sa uplatňovať vo všetkých členských štátoch od 25. mája 2018.

Inštrukcie:

1. *V samostatnom dokumente po konzultácii s poradcom identifikujte IS osobných údajov a ich právne základy.*
2. *Pokúste sa vyplniť priložený dotazník, čo možno najdetailnejšie.*
3. *Prejdite si odpovede na otázky s Vašim poradcom.*
4. *Otázky, ktoré nebudete vedieť zodpovedať, prekonzultujte s Vašim poradcom.*
5. *Zoznam otázok nie je vyčerpávajúci a bol vyhotovený vo všeobecnej rovine.*
6. *Po vyplnení dotazníka a preštudovaní súvisiacej dokumentácie Vám môžu byť položené ďalšie doplňujúce otázky, resp. môžu vyvstať ďalšie otázky.*
7. *V prípade akýchkoľvek otázok sa neváhajte obrátiť na náš GDPR tím.*

Č.	PROBLÉM	OTÁZKY	ODPOVEDE
	VŠEOBECNE O FIRME		
	POČET ZAMESTNANCOV A ORG. ŠTRUKTÚRA	Koľko máte zamestnancov?	441
		Aké máte oddelenia?	
		Prosím priložte organizačnú štruktúru Vašej spoločnosti.	
		Koľko zamestnancov má oddelenie IT a bezpečnosť IT?	38
	POČET INFORMAČNÝCH SYSTÉMOV	Koľko máte informačných systémov, kde sa nachádzajú osobné údaje?	16
	RIADENIE IT	Ako je riadené IT vo vašej spoločnosti, máte zavedené procesy (ITIL, ISO a iné)?	Odbor IKT
		Ako je riadená bezpečnosť vo vašej spoločnosti, máte implementovanú bezpečnostnú politiku, klasifikáciu informácií? (napr. ISO 27 000)	BP áno Klasifikácia informácií = IRA
		Máte bezpečnostného manažéra?	nie
		Máte zavedené v spoločnosti riadenie rizik?	IRA
	GEOGRAFICKÉ ROZLOŽENIE	Aké máte geografické rozmiestnenie spoločnosti všeobecne, ale aj s pohľadu spracovania osobných údajov?	Územie SR
		Z hľadiska vlastníctva ste vo svojich priestoroch alebo priestoroch tretej osoby?	Tretej osoby
A	**OSOBNÉ ÚDAJE**		

1.	**SPRACOVANIE OSOBNÝCH ÚDAJOV**	Spracovávate osobné údaje[1]?	áno
2.		V akých informačných systémoch[2] na spracovanie[3] osobných údajov?	IT
3.		Ktoré z nich majú podobu automatizovaného a neautomatizovaného spracovávania?	Všetky sú IT
4.		Uveďte prosím rozsah osobných údajov, ktoré v jednotlivých informačných systémoch spracúvate?	Rozsahy sú dané v EL IS
5.		Aké sú účely spracovávania osobných údajov v jednotlivých informačných systémoch?	Za účelom verejného záujmu a ochrany života a verejného zdravia + v zmysle zákonov o účtovníctve
6.		Dochádza k prenosu osobných údajov aj mimo SR, do iných krajín v rámci EU/EEA? Uveďte akých.	nie
7.		Dochádza k prenosu osobných údajov aj mimo EÚ?	nie
8.		Ak áno, prosím uveďte akých, z ktorých informačných systémov a či k tomu máte súhlas dotknutej osoby, resp. iný právny základ.	-
9.	**SPRACOVANIE OSOBITNEJ KATEGÓRIE OSOBNÝCH ÚDAJOV**	Spracovávate citlivé osobné údaje (zdravotný stav, biometrické údaje, ...)[4]? Ak áno, uveďte aké a v ktorých informačných systémoch.	áno – IS linky tiesňového volania
10.		Dochádza k prenosu citlivých osobných údajov aj mimo SR, do	nie

---

[1] sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba"); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

[2] je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe.

[3] je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

[4] osobné údaje, ktoré odhaľujú *rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov* na individuálnu identifikáciu fyzickej osoby, *údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.*

		iných krajín v rámci EU/EEA? Uveďte akých.	
11.		Dochádza k prenosu citlivých osobných údajov aj mimo EÚ?	nie
12.		Ak áno, prosím uveďte akých, z ktorých informačných systémov a či k tomu máte súhlas dotknutej osoby.	-
13.	**OSOBNÉ ÚDAJE MALOLETÝCH**	Spracovávate osobné údaje maloletých detí mladších ako 16 rokov? Ak áno uveďte, v akých informačných systémoch.	áno – IS linky tiesňového volania
14.		Máte k takémuto spracovávaniu osobných údajov súhlas zákonných zástupcov?	nie
15.		Ako nakladáte s týmito údajmi a za akým účelom ich spracúvate?	Za účelom verejného záujmu a ochrany života a verejného zdravia
16.		Využívate tieto údaje na vytváranie profilov a v online prostredí pri poskytovaní služieb informačnej spoločnosti?	nie
B	**OBLASŤ PÔSOBNOSTI**		
1.	**EÚ PREVÁDZKOVATEĽ**	Vystupujete v pozícii prevádzkovateľa[5]?	áno – orgán verejnej moci v 15-tich IS
		V ktorých informačných systémoch?	IS JIS HM je prevádzkovateľ VÚJE Trnava
2.		Vymedzujete účel spracúvania samostatne alebo spoločne s ďalším prevádzkovateľom? Ak áno, v akých informačných systémoch.	Samostatne v 15-tich
3.	**EÚ SPROSTREDKOVATEĽ**	Vystupujete v pozícii sprostredkovateľa[6] (spracúvate osobne údaje z poverenia iného prevádzkovateľa)? Ak áno, v akých informačných systémoch.	nie

[5] je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu.

[6] je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.

4.	**SPROSTREDKOVATELIA**	Kto sú Vaši sprostredkovatelia v rámci jednotlivých informačných systémov (napr. externé firmy – dodávatelia služieb, napr. účtovníctvo, IT firmy,...)?	-
5.		Aké všetky služby si outsourcujete, pri ktorých dochádza k spracúvaniu osobných údajov (t.j. iný subjekt má prístup k osobným údajom, za ktoré zodpovedáte alebo nakladá s osobnými údajmi a je potrebné zabezpečiť primeranú úroveň ochrany)?	-
6.	**HLAVNÁ PREVÁDZKAREŇ**[7]	Kde máte Vaše hlavné EÚ HQ? Kde sa prijímajú hlavné rozhodnutia týkajúce sa spracovávania osobných údajov – tzv. hlavná prevádzkareň[8]?	OS ZZS SR, Trnavská cesta 8/A, Bratislava
7.	**PREVÁDZKOVATEĽ SPROSTREDKOVATEĽ MIMO EÚ**	/ Spracovávate osobné údaje v spolupráci so sprostredkovateľmi (subjekty, ktoré konajú z Vášho poverenia) alebo prevádzkovateľmi, ktorí majú sídlo mimo Európskej únie?	nie
8.		Uveďte, na základe akého právneho základu dochádza k prenosu.	-
9.		Spracovávajú nejaké spoločnosti so sídlom mimo Európskej únie údaje o EÚ občanoch vo Vašej skupine podnikov? Zhromažďujú alebo monitorujú ich správanie vo veľkom rozsahu (EÚ	-

[7] Hlavnou prevádzkarňou prevádzkovateľa v Únii by malo byť miesto jeho centrálnej správy v Únii, pokiaľ sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov neprijímajú v inej prevádzkarni prevádzkovateľa v Únii, pričom v takom prípade by sa za hlavnú prevádzkareň mala považovať táto iná prevádzkareň. Hlavná prevádzkareň prevádzkovateľa v Únii by sa mala určiť podľa objektívnych kritérií a mala by zahŕňať efektívne a skutočné vykonávanie riadiacich činností, pri ktorých sa prijímajú hlavné rozhodnutia týkajúce sa účelu a prostriedkov spracúvania prostredníctvom stálych dojednaní. Uvedené kritérium by nemalo byť závislé od toho, či sa spracúvanie osobných údajov vykonáva na tomto mieste. Prítomnosť a použitie technických prostriedkov a technológií spracúvania osobných údajov alebo spracovateľských činností nepredstavujú sami osebe hlavnú prevádzkareň, a preto nie sú určujúcimi kritériami pre hlavnú prevádzkareň. Hlavnou prevádzkarňou sprostredkovateľa by malo byť miesto jeho centrálnej správy v Únii alebo ak v Únii nemá centrálnu správu, tak miesto, kde sa uskutočňujú hlavné spracovateľské činnosti v Únii. V prípadoch týkajúcich sa tak prevádzkovateľa, ako aj sprostredkovateľa by mal príslušným vedúcim dozorným orgánom zostať dozorný orgán členského štátu, v ktorom má prevádzkovateľ svoju hlavnú prevádzkareň, ale dozorný orgán sprostredkovateľa by sa mal považovať za dotknutý dozorný orgán a uvedený dozorný orgán by sa mal zúčastňovať na postupe spolupráce stanovenom v tomto nariadení. V každom prípade dozorné orgány členského štátu alebo členských štátov, v ktorých má sprostredkovateľ jednu alebo viac prevádzkarní, by sa nemali považovať za dotknuté dozorné orgány, ak sa návrh rozhodnutia týka len prevádzkovateľa. **Ak spracúvanie vykonáva skupina podnikov, hlavná prevádzkareň riadiaceho podniku by sa mala považovať za hlavnú prevádzkareň skupiny podnikov okrem prípadu, keď o účeloch a prostriedkoch spracúvania rozhoduje iný podnik.**

[8] pokiaľ ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, miesto jeho centrálnej správy v Únii s výnimkou prípadu, keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Únii a táto iná prevádzka má právomoc presadiť vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje prevádzkareň, ktorá takéto rozhodnutia prijala.

		občanov)?	
10.		Ak áno, vymenovali tieto zahraničné spoločnosti zástupcu[9] v rámci Európskej únie?	-
11.		Uskutočnili vymenovanie v písomnej forme?	-
12.		Je tento zástupca v EÚ poverený, aby bol kontaktovaný Úradom a dotknutými osobami v súvislosti s problematickými otázkami pri spracovaní osobných údajov ako prvé kontaktné miesto?	nie
13.	**SPOLOČNÍ PREVÁDZKOVATELIA**	Vykonávate nejaké spracovateľské operácie s osobnými údajmi ako spoloční prevádzkovatelia[10] jedného informačného systému?	nie
14.		Ak áno uveďte, v ktorých informačných systémoch.	-
C	**ZÁKONNOSŤ SPRACÚVANIA / PRÁVNY ZÁKLAD**		
1.	**PRÁVNY ZÁKLAD[11]**	Viete identifikovať právny základ spracúvania v súčasných	§10 ods.3 písm. c) a g) zákona 122/2013 Z.z. o

[9] Ak prevádzkovateľ alebo sprostredkovateľ, ktorý nie je usadený v Únii, spracúva osobné údaje dotknutých osôb, ktoré sa nachádzajú v Únii, pričom jeho spracovateľské činnosti súvisia s ponukou tovaru alebo služieb takýmto dotknutým osobám v Únii, bez ohľadu na to, či sa od dotknutej osoby vyžaduje platba, alebo so sledovaním ich správania sa, pokiaľ sa toto ich správanie uskutočňuje v Únii, prevádzkovateľ alebo sprostredkovateľ by mal určiť zástupcu **okrem prípadov, keď spracúvanie, ktoré vykonáva, je občasné, nezahŕňa vo veľkom rozsahu spracúvanie osobitných kategórií osobných údajov alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky, a nie je pravdepodobné, že povedie k riziku pre práva a slobody fyzických osôb**, pričom sa zohľadní povaha, kontext, rozsah a účely spracúvania, alebo **keď je prevádzkovateľ orgánom verejnej moci alebo verejnoprávnym subjektom**. Zástupca by mal konať v mene prevádzkovateľa alebo sprostredkovateľa a môže sa na neho obracať ktorýkoľvek dozorný orgán. Zástupca by mal byť výslovne určený písomným poverením prevádzkovateľa alebo sprostredkovateľa, aby konal v jeho mene v súvislosti s jeho povinnosťami podľa tohto nariadenia. Určenie takého zástupcu neovplyvňuje zodpovednosť alebo povinnosť prevádzkovateľa alebo sprostredkovateľa podľa tohto nariadenia. Takýto zástupca by mal vykonávať svoje úlohy podľa poverenia, ktoré dostal od prevádzkovateľa alebo sprostredkovateľa a ktoré zahŕňa spoluprácu s príslušnými dozornými orgánmi v súvislosti s opatreniami prijatými na zabezpečenie súladu s týmto nariadením. V prípade, že prevádzkovateľ alebo sprostredkovateľ nezabezpečia súlad, určený zástupca by mal podliehať konaniam na presadenie práva.

[10] Ak dvaja alebo viacerí prevádzkovatelia spoločne určia účely a prostriedky spracúvania, sú spoločnými prevádzkovateľmi.

[11] Spracúvanie je zákonné iba vtedy a iba v tom rozsahu, keď je splnená aspoň jedna z týchto podmienok:
a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov na jeden alebo viaceré konkrétne účely;
b) spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy;
c) spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa;
d) spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby;
e) spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;

		informačných systémoch? Prosím uveďte.	OOÚ zákon č. 579/2004 o záchrannej zdravotnej službe
2.		Disponujete právnym základom pre spracovanie osobných údajov vo vzťahu ku každej spracovateľskej operácii vo Vašej spoločnosti, ktorú vykonávate?	áno
3.		Disponujete právnym základom pre spracovanie citlivých osobných údajov[12]?	áno
4.	**SÚHLAS DOTKNUTEJ OSOBY[13]**	V ktorých informačných systémoch sú osobné údaje spracúvané	IS školenia prvej pomoci pre zdravotníckych pracovníkov

---

f) spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobou dieťa.

[12] Zákaz spracúvania citlivých osobných údajov sa neuplatňuje, ak platí niektorá z týchto podmienok:

a) dotknutá osoba vyjadrila **výslovný súhlas so spracúvaním** týchto osobných údajov na jeden alebo viacero určených účelov, s výnimkou prípadov, keď sa v práve Únie alebo v práve členského štátu stanovuje, že zákaz uvedený v odseku 1 nemôže dotknutá osoba zrušiť;

b) spracúvanie je **nevyhnutné na účely plnenia povinností a výkonu osobitných práv** prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva a práva sociálneho zabezpečenia a sociálnej ochrany, pokiaľ je to povolené právom Únie alebo právom členského štátu alebo kolektívnou zmluvou podľa práva členského štátu poskytujúcimi primerané záruky ochrany základných práv a záujmov dotknutej osoby;

c) spracúvanie je nevyhnutné **na ochranu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby** v prípade, že dotknutá osoba nie je fyzicky alebo právne spôsobilá vyjadriť svoj súhlas;

d) spracúvanie vykonáva v rámci svojej zákonnej činnosti s primeranými zárukami nadácia, združenie alebo akýkoľvek iný neziskový subjekt s politickým, filozofickým, náboženským alebo odborárskym zameraním a pod podmienkou, že spracúvanie sa týka výlučne členov alebo bývalých členov subjektu alebo osôb, ktoré majú pravidelný kontakt s ním v súvislosti s jeho cieľmi, a že bez súhlasu dotknutej osoby sa osobné údaje neposkytnú mimo tohto subjektu;

e) spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila;

f) spracúvanie je nevyhnutné na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo kedykoľvek, keď súdy vykonávajú svoju súdnu právomoc;

g) spracúvanie je nevyhnutné z dôvodov významného verejného záujmu na základe práva Únie alebo práva členského štátu, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu údajov a stanovujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby;

h) spracúvanie je nevyhnutné na účely preventívneho alebo pracovného lekárstva, posúdenia pracovnej spôsobilosti zamestnanca, lekárskej diagnózy, poskytovania zdravotnej alebo sociálnej starostlivosti alebo liečby, alebo riadenia systémov a služieb zdravotnej alebo sociálnej starostlivosti na základe práva Únie alebo práva členského štátu alebo podľa zmluvy so zdravotníckym pracovníkom, a podlieha podmienkam a zárukám uvedeným v odseku 3;

i) spracúvanie je nevyhnutné z dôvodov verejného záujmu v oblasti verejného zdravia, ako je ochrana proti závažným cezhraničným ohrozeniam zdravia alebo zabezpečenie vysokej úrovne kvality a bezpečnosti zdravotnej starostlivosti a liekov alebo zdravotníckych pomôcok, na základe práva Únie alebo práva členského štátu, ktorým sa stanovujú vhodné a konkrétne opatrenia na ochranu práv a slobôd dotknutej osoby, najmä profesijné tajomstvo;

j) spracúvanie je nevyhnutné na účely archivácie vo verejnom záujme, alebo na účely vedeckého alebo historického výskumu či na štatistické účely podľa článku 89 ods. 1 na základe práva Únie alebo práva členského štátu, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu údajov a určujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby.

[13] akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka.

		na základe súhlasu dotknutej osoby?	IS školenia prvej pomoci pre laikov
5.		Akým spôsobom je tento súhlas získavaný? Akým spôsobom je súhlas vyjadrený? *(Ak je aplikovateľné, prosím predložte formuláciu tohto súhlasu.)*	V súlade so znením §11 zákona č. 122/2013
6.		Je súhlas zachytený takým spôsobom, že umožňuje v prípade kontroly Úradu preukázať skutočnosť, že dotknutá osoba udelila prevádzkovateľovi súhlas so spracovaním osobných údajov slobodne, dobrovoľne a určito?	áno
7.		Je možné udelený súhlas odvolať?	áno
8.		Ak áno, akým spôsobom? Je tento spôsob rovnako jednoduchý, ako udelenie súhlasu? Ak nie, prečo.	áno
D	**TRANSPARENTNOSŤ SPRACÚVANIA**		
1.	**SPLNENIE NOTIFIKAČNEJ POVINNOTI VO VZŤAHU K DOTKNUTÝM OSOBÁM**	Sú dotknuté osoby informované o spôsobe spracovania? Akým spôsobom? *Prosím predložte k nahliadnutiu dokument, ktorým si plníte notifikačnú povinnosť voči dotknutým osobám za účelom posúdenia splnenia rozsahu notifikačnej povinnosti.*	nie
2.	**ZDROJ, Z KTORÉHO SÚ ZÍSKAVANÉ OSOBNÉ ÚDAJE A ROZSAH INFORMÁCIÍ, KTORÉ SÚ POSKYTOVANÉ DOTKNUTÝM OSOBÁM**	Sú osobné údaje zhromažďované priamo od dotknutých osôb alebo z iného zdroja/od tretej osoby?	Od dotknutých osôb
3.		Poskytujete ako prevádzkovateľ / sprostredkovateľ dotknutým osobám informácie v Nariadením ustanovenom rozsahu? Ak neviete odpovedať, prosím uveďte aké informácie v súčasnosti poskytujete alebo predložte príslušný dokument.	Neposkytujeme
4.		Sú osobné údaje získané inak ako priamo od dotknutej osoby?	Od osoby volajúcej na LTV
5.		Sú v tomto prípade dotknutým osobám poskytované Nariadením vyžadované informácie v súlade so zásadou transparentnosti? Ak neviete odpovedať, prosím uveďte aké informácie v súčasnosti poskytujete.	nie

E	SPRACÚVANIE V SÚLADE SO ZÁSADAMI SPRACÚVANIA[14]		
1.	LIMITÁCIA ÚČELU SPRACÚVANIA	Sú osobné údaje spracovávané výlučne v súlade s účelom, na ktorý boli získané?	áno
2.	MINIMALIZÁCIA SPRACOVANIE OSOBNÝCH ÚDAJOV	Sú spracovávané výlučne osobné údaje nevyhnutné na dosiahnutie účelu, za ktorým boli zhromaždené?	áno
3.		Je potrebné na jednotlivé účely spracovávať všetky kategórie osobných údajov, ktoré v súčasnosti spracovávate?	áno
4.		Je možné niektoré z osobných údajov, ktoré v súčasnosti spracovávate, vymazať z dôvodu nepotrebnosti/nadbytočnosti?	O tom rozhodujú vlastníci IS
5.	PRESNOSŤ A SPRÁVNOSŤ	Sú zavedené interné politiky a sú vykonané tréningy / školenia za účelom zabezpečenia kontroly správnosti spracovávaných osobných údajov?	IRA sú zavedené Nevzdeláva sa
6.		V prípade, ak je zistené, že spracovávané osobné údaje sú nepresné / nesprávne je vykonaná náprava bez zbytočného odkladu?	áno

[14] Osobné údaje musia byť:
a) spracúvané **zákonným spôsobom, spravodlivo a transparentne** vo vzťahu k dotknutej osobe („zákonnosť, spravodlivosť a transparentnosť"");
b) získavané na **konkrétne určené, výslovne uvedené a legitímne účely** a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi; ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely sa v súlade s článkom 89 ods. 1 nepovažuje za nezlučiteľné s pôvodnými účelmi („obmedzenie účelu");
c) **primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú** („minimalizácia údajov");
d) správne a podľa potreby **aktualizované**; musia sa prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia („správnosť"");
e) uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú; osobné údaje sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely v súlade s článkom 89 ods. 1 za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných týmto nariadením na ochranu práv a slobôd dotknutých osôb („minimalizácia uchovávania");
f) spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení („integrita a dôvernosť").

7.		Akým spôsobom prebieha proces kontroly a následnej opravy?	Verifikáciou v procese získavania OÚ a
8.	**MINIMALIZÁCIA / OBMEDZENIE UCHOVÁVANIA OSOBNÝCH ÚDAJOV**	Majú interné politiky týkajúce sa osobných údajov zahrnuté aj informácie týkajúce sa uchovávania / ukladania / zálohovania osobných údajov (popis procesov / doby uchovávania)?	áno
9.		Akým spôsobom prebieha zálohovanie?	Odbor IKT
10.		Sú zavedené procesy, ktoré zabezpečujú archiváciu osobných údajov?	áno
11.		V krátkosti popíšte, ako prebieha archivácia / zálohovanie vo Vašej organizácii.	Odbor IKT
12.		Sú zavedené procedúry, ktoré sú spôsobilé zabezpečiť výmaz osobných údajov? Ako často sú kontrolované osobné údaje?	áno
13.		Ako často je zabezpečovaný výmaz osobných údajov? Akým spôsobom prebieha likvidácia osobných údajov?	Odbor IKT
14.	**INTEGRITA A DÔVERNOSŤ**	Sú zavedené primerané bezpečnostné opatrenia, ktoré zabezpečujú dostatočnú / primeranú ochranu osobných údajov?	áno
15.		Ako často prehodnocujete bezpečnostnú politiku a ako často sú implementované nové riešenia do existujúcej infraštruktúry?	Priebežne podľa potreby
16.	**ZODPOVEDNOSŤ ZA SPRACOVANIE OSOBNÝCH ÚDAJOV**	Je Vaša spoločnosť schopná preukázať dôkazmi či už listinnými alebo softvérovými, že je v súlade s požiadavkami Nariadenia?	áno
F	**PRÁVA DOTKNUTÝCH OSÔB**		
1.	**ZABEZPEČENIE PRÍSTUPU K OSOBNÝM ÚDAJOM[15]**	Máte písomne spracované politiky / procedúry na spracovanie žiadostí dotknutých osôb o prístup k osobným údajom, ktoré sú	áno

[15] 1. Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má právo získať prístup k týmto osobným údajom a tieto informácie:
a) účely spracúvania;

		o ich osobe spracúvané?	
2.		Majú dotknuté osoby k dispozícii mechanizmus implementovaný v rámci organizácie, ktorý má zabezpečiť spracovávanie žiadostí o prístup k informáciám, ktoré sú o ich osobe spracovávané?	áno
3.		Ste schopní reagovať na žiadosti o poskytnutie informácie v lehote jedného mesiaca? Máte určenú osoby zodpovedné za uvedené?	áno
4.		V prípade, ak tieto údaje spracováva sprostredkovateľ v mene Vašej spoločnosti, je sprostredkovateľ schopný reagovať na žiadosti o poskytnutie informácie v lehote jedného mesiaca?	Nemáme
5.	**PRENOSNOSŤ OSOBNÝCH ÚDAJOV**[16]	Môžu dotknuté osoby získať svoje osobné údaje v štruktúrovanej, bežne používanej strojovo čitateľnej podobe / formáte?	áno
6.		Máte zavedené procedúry na ich vybavenie?	áno
7.	**PRÁVO NA VÝMAZ**[17]	Sú dotknuté osoby informované o ich práve žiadať výmaz alebo	nie

---

b) kategórie dotknutých osobných údajov;
c) príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie;
d) ak je to možné, predpokladaná doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;
e) existencia práva požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti takémuto spracúvaniu;
f) právo podať sťažnosť dozornému orgánu;
g) ak sa osobné údaje nezískali od dotknutej osoby, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj;
h) existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a v týchto prípadoch aspoň zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.
2. Ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii, dotknutá osoba má právo byť informovaná o primeraných zárukách podľa článku 46 týkajúcich sa prenosu.
3. Prevádzkovateľ poskytne kópiu osobných údajov, ktoré sa spracúvajú. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob.
4. Právo získať kópiu uvedenú v odseku 3 nesmie mať nepriaznivé dôsledky na práva a slobody iných.
[16] Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto údaje ďalšiemu prevádzkovateľovi bez toho, aby jej prevádzkovateľ, ktorému sa tieto osobné údaje poskytli, bránil, ak:
a) sa spracúvanie zakladá na súhlase, alebo na zmluve, a
b) ak sa spracúvanie vykonáva automatizovanými prostriedkami.

		práve na opravu osobných údajov, ktoré sú o nich spracovávané (ak je právo na výmaz aplikovateľné)?	
8.		Sú u Vás zavedené kontrolné a formálne mechanizmy / procedúry, ktoré umožňujú, aby boli osobné údaje o konkrétnej dotknutej osobe vymazané alebo blokované?	áno
9.		Sú príslušné procedúry schopné vyhovieť takýmto žiadostiam? Je potrebné ich prispôsobiť?	áno
10.	**PRÁVO NAMIETAŤ SPRACOVANIE**	Sú dotknuté osoby informované o práve namietať vo vzťahu k vybraným typom spracovania?	nie
11.		Sú prijaté politiky, ktoré majú zabezpečiť, že právu namietať spracovanie osobných údajov, bude účinne vyhovené, resp. bude spracované?	nie
12.	**PROFILOVANIE A AUTOMATICKÉ SPRACOVANIE**	Vykonávate vo Vašej spoločnosti automatické spracovávanie/profilovanie osobných údajov, resp. štatistické vyhodnocovanie?	áno
13.		Je profilovanie (ako spôsob spracovávania – štatistické spracovávanie údajov o dotknutých osobách) založené na súhlase dotknutej osoby?	nie
14.		Je tento súhlas výslovný / explicitný? Viete ho preukázať?	-
15.		Spracovávate v rámci profilovania aj citlivé osobné údaje?	áno

---

[17] Dotknutá osoba má tiež právo dosiahnuť u prevádzkovateľa bez zbytočného odkladu vymazanie osobných údajov, ktoré sa jej týkajú, a prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak je splnený niektorý z týchto dôvodov:
a) osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali;
b) dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva, a ak neexistuje iný právny základ pre spracúvanie;
c) dotknutá osoba namieta voči spracúvaniu na účely úlohy realizovanej vo verejnom záujme, oprávnených záujmov, profilovania/priameho marketingu a neprevažujú žiadne oprávnené dôvody na spracúvanie alebo dotknutá osoba namieta voči tomuto spracúvaniu;
d) osobné údaje sa spracúvali nezákonne;
e) osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha;
f) osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti.

16.		Spracovávate v rámci profilovania aj údaje o deťoch? Aj citlivé osobné údaje o deťoch?	áno
G	**BEZPEČNOSTNÉ INCIDENTY**		
1.	**POVINNOSŤ REAGOVAŤ NA BEZPEČNOSTNÉ INCIDENTY[18]**	Máte v rámci spoločnosti zdokumentovaný proces, ako postupovať v prípade bezpečnostného incidentu?	áno
2.		Máte zavedený systém na identifikáciu bezpečnostných incidentov aj vo forme softvérového riešenia?	áno
3.		Máte pripravený reakčný plán na riešenie bezpečnostných incidentov?	áno
4.		Sú reakčný plán a implementované mechanizmy pravidelne kontrolované / prehodnocované a testované?	nie
5.		Sú výsledky testov zdokumentované?	nie
6.		Máte vo Vašej spoločnosti vnútorný predpis, ktorý upravuje postup pri nahlasovaní bezpečnostných incidentov interne osobe zodpovednej za ochranu osobných údajov v spoločnosti?	áno
7.		Máte nastavené a implementované procesy na rýchle nahlasovanie bezpečnostných incidentov Úradu a dotknutým osobám? Máte implementovaný vhodný softvér?	nie
8.		Máte vo Vašej spoločnosti spracovaný vnútorný predpis, ktorý vysvetľuje, ktoré informácie, resp. bezpečnostné incidenty musia byť nahlasované Úradu a ktoré dotknutým osobám a za akých	áno

[18] V prípade porušenia ochrany osobných údajov prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámi porušenie ochrany osobných údajov dozornému orgánu s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb. Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania.

		podmienok? Špecifikuje predpis i informácie, ktoré sa nahlasujú a ktoré nie? [19]	
9.		Ak využívate sprostredkovateľov, máte zavedenú procedúru / mechanizmus, na základe ktorého je Sprostredkovateľ povinný vo vopred určenej forme nahlasovať bezpečnostné incidenty prevádzkovateľovi bez akéhokoľvek omeškania po tom, čo sa o incidente dozvedel?	-
10.		Je táto povinnosť reflektovaná aj v zmluve so sprostredkovateľom? *Za účelom overenia prosím predložte zmluvy s Vašimi sprostredkovateľmi.*	-
11.		Máte zabezpečené dokumentovanie bezpečnostných incidentov?	áno
12.		Máte zavedený špeciálny model spolupráce ako spoločne postupovať pri zvládnutí bezpečnostných incidentov medzi Vašimi sprostredkovateľmi, dodávateľmi a ďalšími partnermi?	-
13.		Zvážili ste prípadné poistenie zodpovednosti za porušenie povinnosti pri bezpečnostných incidentoch? *(V zmysle Nariadenia nie je povinné).*	Toto je v kompetencii štatutára
H	**ĎALŠIE POVINNOSTI PREVÁDZKOVATEĽA**		
1.	**TECHNICKÉ A ORGANIZAČNÉ OPATRENIA**	Aké školenia poskytujete svojim zamestnancom v oblasti ochrany osobných údajov?	V súčasnej dobe sa neškolia

[19] Oznámenie musí obsahovať musí obsahovať aspoň:
a) opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch;
b) meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií;
c) opis pravdepodobných následkov porušenia ochrany osobných údajov;
d) opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

2.		Vediete o školeniach záznamy?	Viedli sme do roku 2016
3.		Máte podpísané aktuálne poučenia oprávnených osôb?	áno
4.		Máte vo Vašej spoločnosti jasne zdokumentované interné politiky a procedúry, ktoré preukazujú súlad s požiadavkami Nariadenia?	nie
5.		Vykonávate pravidelný audit, aby ste preverili dostatočnosť prijatých technických a organizačných opatrení?	čiastočne
6.	**PRIVACY BY DESIGN & DEFAULT**[20]	Máte interné politiky a procesy nastavené tak, aby integrovali požiadavku na kontinuálne prehodnocovanie súladu s požiadavkami Nariadenia?	nie
7.	**ZODPOVEDNÁ OSOBA**	Máte povinnosť vymenovať zodpovednú osobu v zmysle informácii z úvodného školenia?[21]	V súčasnosti je menovaná ZO ale jej menovanie končí 24.mája 2018
8.		Mali ste doteraz vymenovanú zodpovednú osobu v zmysle zákona o ochrane osobných údajov?	áno
9.		Ohlasovali ste ju na Úrad?	áno
10.		Ak nie je vymenovanie zodpovednej osoby Vašou povinnosťou v zmysle Nariadenia, prosím prehodnoťte či k menovaniu zodpovednej osoby nepristúpite na dobrovoľnej báze.	-

[20] So zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb, prevádzkovateľ v čase určenia prostriedkov spracúvania aj v čase samotného spracúvania prijme primerané technické a organizačné opatrenia, ako je napríklad **pseudonymizácia**, ktoré sú určené na účinné zavedenie zásad ochrany údajov, ako je minimalizácia údajov, a začlení do spracúvania nevyhnutné záruky s cieľom splniť požiadavky tohto nariadenia a chrániť práva dotknutých osôb. Prevádzkovateľ vykoná primerané technické a organizačné opatrenia, aby zabezpečil, že štandardne sa spracúvajú len osobné údaje, ktoré sú nevyhnutné pre každý konkrétny účel spracúvania. Uvedená povinnosť sa vzťahuje na množstvo získaných osobných údajov, rozsah ich spracúvania, dobu ich uchovávania a ich dostupnosť. Konkrétne sa takýmito opatreniami zabezpečí, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.

[21] Povinnosť ustanoviť zodpovednú osobu má prevádzkovateľ a sprostredkovateľ vtedy, ak
a)spracúvanie vykonáva orgán verejnej moci s výnimkou súdov pri výkone ich súdnej právomoci;
b)hlavnými činnosťami sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu; alebo
c)hlavnými činnosťami je spracúvanie osobitných kategórií údajov vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky.

11.		V rámci skupiny podnikov môže byť menovaná jedna zodpovedná osoba.	-
12.		Ak máte menovanú zodpovednú osobu, máte implementované procesy na ohlasovanie incidentov zamestnancami zodpovednej osobe?	nie
13.		Ako je nastavená reportovacia povinnosť zodpovednej osoby vo vzťahu k štatutárom spoločnosti?	IRA
14.		Ak sa jedná o interného zamestnanca, je jeho postavenie v organizačnej štruktúre zaradené tak, aby bol v priamej riadiacej pôsobnosti štatutárov?	nie
15.		Vykonáva u Vás činnosť zodpovednej osoby externá spoločnosť/externý subjekt?	nie
16.		Máte zavedené mechanizmy na priame reportovanie medzi zodpovednou osobou a štatutárnym orgán?	IRA
17.	**PREUKAZOVANIE SÚLADU A VEDENIE ZÁZNAMOV[22]**	Koľko zamestnancov má Vaša spoločnosť?	441

[22] Každý prevádzkovateľ a v príslušnom prípade zástupca prevádzkovateľa vedie záznamy o spracovateľských činnostiach, za ktoré je zodpovedný. Tieto záznamy musia obsahovať všetky tieto informácie:
a) meno/názov a kontaktné údaje prevádzkovateľa a v príslušnom prípade spoločného prevádzkovateľa, zástupcu prevádzkovateľa a zodpovednej osoby;
b) účely spracúvania;
c) opis kategórií dotknutých osôb a kategórií osobných údajov;
d) kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, vrátane príjemcov v tretích krajinách alebo medzinárodných organizáciách;
e)v príslušných prípadoch prenosy osobných údajov do tretej krajiny alebo medzinárodnej organizácii vrátane označenia predmetnej tretej krajiny alebo medzinárodnej organizácie a v prípade prenosov uvedených vo výnimkách pri prenosoch podľa článku 49 ods. 1 druhom pododseku dokumentáciu primeraných záruk;
f) podľa možností predpokladané lehoty na vymazanie rôznych kategórií údajov;
g) podľa možností všeobecný opis technických a organizačných bezpečnostných opatrení.
Každý sprostredkovateľ a v príslušnom prípade zástupca sprostredkovateľa vedie záznamy o všetkých kategóriách spracovateľských činností, ktoré vykonal v mene prevádzkovateľa, pričom tieto záznamy obsahujú:
a) meno/názov a kontaktné údaje sprostredkovateľa alebo sprostredkovateľov a každého prevádzkovateľa, v mene ktorého sprostredkovateľ koná, a v príslušnom prípade zástupcu prevádzkovateľa alebo sprostredkovateľa a zodpovednej osoby;
b) kategórie spracúvania vykonávaného v mene každého prevádzkovateľa;

18.		Disponujete právnymi základmi pre spracovanie takýchto údajov a viete tieto právne základy preukázať v dokumentovateľnej forme?	áno
19.	**ANALÝZA – POSÚDENIE VPLYVOV[23]**	Máte zavedené procesy na identifikáciu potreby vypracovania analýzy vplyvov a postupy vypracovania analýzy vplyvov?	nie
20.		Máte povinnosti týkajúce sa vykonávania posúdenia vplyvov premietnuté aj v sprostredkovateľských zmluvách?	-
21.	**PREVIERKY SPROSTREDKOVATEĽOV**	Vykonávate predchádzajúcu previerku servisných dodávateľov a vediete záznamy o vykonanej previerke?	-
I	**PRENOSY OSOBNÝCH ÚDAJOV MIMO EÚ/EEA**		
1.	**MAPOVANIE CEZHRANIČNÉHO TOKU**	Sú osobné údaje prenášané mimo EÚ / EEA? Ak áno, do ktorých krajín?	nie
2.		Aké typy osobných údajov sú prenášané? Vymenujte prosím rozsah prenášaných údajov / právny základ Zahŕňajú prenášané údaje aj citlivé osobné údaje?	-
3.		Aké sú účely cezhraničného prenosu?	-
4.		Sú všetky cezhraničné prenosy riadne dokumentované?	-

---

c) v príslušných prípadoch prenosy osobných údajov do tretej krajiny alebo medzinárodnej organizácii vrátane označenia predmetnej tretej krajiny alebo medzinárodnej organizácie a v prípade prenosov uvedených v článku 49 ods. 1 druhom pododseku dokumentáciu primeraných záruk;
d) podľa možností všeobecný opis technických a organizačných bezpečnostných opatrení.
Záznamy sa vedú v písomnej podobe vrátane elektronickej podoby.
Povinnosti viesť záznamy sa nevzťahujú na podnik alebo organizáciu, ktorá zamestnáva menej ako 250 osôb, pokiaľ nie je pravdepodobné, že spracúvanie, ktoré vykonáva, povedie k riziku pre práva a slobody dotknutej osoby, pokiaľ je toto spracúvanie príležitostné alebo nezahŕňa citlivé osobné údajov alebo osobných údajov týkajúcich sa uznaní viny za trestné činy a priestupky.
[23] Posúdenie vplyvu sa vyžaduje v situáciách:
a)systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené **na automatizovanom spracúvaní** vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu;
b)spracúvania vo veľkom rozsahu osobitných kategórií údajov alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky, alebo
c)systematického monitorovania verejne prístupných miest vo veľkom rozsahu.

5.			Obsahujú evidované informácie o rozsahu prenášaných údajov, o odosielateľovi a príjemcovi, o účele spracúvania, informáciu, z ktorej krajiny do ktorej prebieha export údajov, informáciu o tom, kto je prijímateľom týchto osobných údajov?	-
6.			Sú právne záruky a primerané mechanizmy pre každý cezhraničný prenos určené a zdokumentované?	-
7.	OPRÁVNENOSŤ CEZHRANIČNÝCH PRENOSOV		Sú všetky transfery do zahraničia pokryté primeranými mechanizmami (záväzné vnútropodnikové pravidlá, štandardné zmluvné doložky, súhlas dotknutej osoby, privacy shield) alebo výnimkami?	-
8.	TRANSPARENTNOSŤ		Sú dotknuté osoby informované o skutočnosti, že dochádza k cezhraničnému prenosu osobných údajov? Ak áno, v akom rozsahu.	-
9.			V akom časovom momente sú tieto skutočnosti oznamované dotknutým osobám? Akým spôsobom je táto informácia poskytovaná dotknutým osobám?	-
10.	CEZHRANIČNÉ PRENOSY VYKONANÉ NA ŽIADOSŤ ORGÁNOV VEREJNEJ MOCI POCHÁDZAJÚCICH Z TRETÍCH KRAJÍN:		Máte spracovaný interný predpis na nakladanie so žiadosťami o sprístupnenie alebo prenos osobných údajov zahraničných orgánov?	áno
J	**KONTROLA PLNENIA POVINNOSTÍ VÁŠHO SPROSTREDKOVATEĽA[24]**			

[24] V súvislosti so spracúvaním, ktoré má v mene prevádzkovateľa vykonať sprostredkovateľ, **by mal prevádzkovateľ pri poverovaní sprostredkovateľa spracovateľskými činnosťami využívať len takých sprostredkovateľov, ktorí poskytujú dostatočné záruky, najmä pokiaľ ide o odborné znalosti, spoľahlivosť a zdroje, na to, že prijmú technické a organizačné opatrenia, ktoré budú spĺňať požiadavky tohto nariadenia, vrátane požiadavky na bezpečnosť spracúvania**. Dodržiavanie schváleného kódexu správania alebo schváleného certifikačného mechanizmu sprostredkovateľom sa môže použiť ako prvok na preukázanie súladu s povinnosťami prevádzkovateľa. **Vykonávanie spracúvania sprostredkovateľom by sa malo riadiť zmluvou alebo iným právnym aktom podľa práva Únie alebo práva členského štátu, ktorými by bol sprostredkovateľ viazaný voči prevádzkovateľovi a v ktorých by sa stanovil predmet a doba spracúvania, povaha a účely spracúvania, typ osobných údajov a kategórie dotknutých osôb, a ktoré by mali zohľadniť osobitné úlohy a povinnosti sprostredkovateľa v kontexte spracúvania, ktoré sa má vykonať, a riziko pre práva a slobody dotknutých osôb**. Prevádzkovateľ a sprostredkovateľ si môžu vybrať použitie individuálnej zmluvy alebo štandardných zmluvných doložiek, ktoré prijme buď priamo Komisia, alebo ktoré prijme dozorný orgán v súlade s mechanizmom konzistentnosti a následne ich prijme Komisia. **Po ukončení spracúvania v mene prevádzkovateľa by mal sprostredkovateľ podľa rozhodnutia prevádzkovateľa vrátiť alebo vymazať osobné údaje, pokiaľ podľa práva Únie alebo práva členského štátu, ktorému sprostredkovateľ podlieha, neexistuje požiadavka na uchovanie osobných údajov.**

1.	**ZMLUVY SO SPROSTREDKOVATEĽMI**	Obsahujú Vaše zmluvy medzi prevádzkovateľom a sprostredkovateľom všetky povinné náležitosti v zmysle Nariadenia?[25]	-
		Viete nám označiť okruh Vašich sprostredkovateľov a zároveň predložiť k nahliadnutiu zmluvy so sprostredkovateľmi za účelom posúdenia.	
		Obsahujú odporúčané oblasti úpravy v zmysle úvodného školenia?	
2.	**POUŽÍVANIE SUB-SPROSTREDKOVATEĽOV**	Máte v zmluve so sprostredkovateľom výslovné písomné splnomocnenie oprávňujúce sprostredkovateľov používať existujúcich sub-sprostredkovateľov?	-
3.		Existujú takéto autorizácie vo vzťahu ku každému navrhovanému spracovaniu osobných údajov sub-sprostredkovateľom?	-
4.		Bola poskytnutá všeobecná alebo špecifická (ku konkrétnemu subjektu) autorizácia?	-
5.		Ak je poskytnutá generálna autorizácia, je zavedený mechanizmus priameho informovania prevádzkovateľa o akýchkoľvek zmenách v štruktúre sub-sprostredkovateľov?	-

---

[25] Zmluva so sprostredkovateľom stanoví najmä predmet a dobu spracúvania, povahu a účel spracúvania, typ osobných údajov a kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa a sprostredkovateľa, ako aj že sprostredkovateľ
a) spracúva osobné údaje len na základe zdokumentovaných pokynov prevádzkovateľa, a to aj pokiaľ ide o prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii,
b) zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú dôvernosť informácií, alebo aby boli viazané vhodnou povinnosťou zachovávať dôvernosť informácií vyplývajúcou zo štatútu;
c) vykoná všetky požadované bezpečnostné opatrenia podľa článku 32;
d) dodržiava podmienky zapojenia ďalšieho sprostredkovateľa;
e) po zohľadnení povahy spracúvania v čo najväčšej miere pomáha prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby;
f) pomáha prevádzkovateľovi zabezpečiť plnenie povinností podľa článkov 32 až 36 (bezpečnostné opatrenia, oznámenie porušenia ochrany osobných údajov dozornému orgánu, posúdenie vplyvov, konzultácia s Úradom) s prihliadnutím na povahu spracúvania a informácie dostupné sprostredkovateľovi;
g) po ukončení poskytovania služieb týkajúcich sa spracúvania na základe rozhodnutia prevádzkovateľa všetky osobné údaje vymaže alebo vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov;
h) poskytne prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia povinností stanovených v tomto článku a umožní audity, ako aj kontroly vykonávané prevádzkovateľom alebo iným audítorom, ktorého poveril prevádzkovateľ, a prispieva k nim.

6.		Sú všetky subjekty, ktoré vykonávajú akékoľvek spracovateľské operácie v mene Vašej spoločnosti ako prevádzkovateľa zmluvnou stranou zmluvy zahŕňajúcou špecifické podmienky spracovania ochrany osobných údajov vo Vašej spoločnosti?	-
7.		Sú premietnuté všetky zmluvné podmienky a povinnosti sprostredkovateľa zo zmluvy so sprostredkovateľom do zmluvy so sub-sprostredkovateľmi? *Prosím overiť.*	-
8.	**PREUKAZOVANIE SÚLADU (VEDENIE ZÁZNAMOV)[26]**	Koľko zamestnancov má spoločnosť sprostredkovateľa?[27]	-
9.		Disponuje sprostredkovateľ právnymi základmi pre spracovanie takýchto údajov a vie tieto právne základy preukázať v dokumentovateľnej forme?	-
10.	**ZODPOVEDNÁ OSOBA**	Majú Vaši sprostredkovatelia povinnosť vymenovať zodpovednú osobu v zmysle informácii z úvodného školenia? Ak áno, majú ju vymenovanú? Mali Vaši sprostredkovatelia doteraz vymenovanú zodpovednú osobu?	-
11.		Ak má sprostredkovateľ menovanú zodpovednú osobu, má implementované procesy na ohlasovanie incidentov zamestnancami zodpovednej osobe/ prevádzkovateľovi?	-
12.		Ako je nastavená reportovacia povinnosť sprostredkovateľa voči	-

---

[26] Každý sprostredkovateľ a v príslušnom prípade zástupca sprostredkovateľa vedie záznamy o všetkých kategóriách spracovateľských činností, ktoré vykonal v mene prevádzkovateľa, pričom tieto záznamy obsahujú:
a) meno/názov a kontaktné údaje sprostredkovateľa alebo sprostredkovateľov a každého prevádzkovateľa, v mene ktorého sprostredkovateľ koná, a v príslušnom prípade zástupcu prevádzkovateľa alebo sprostredkovateľa a zodpovednej osoby;
b) kategórie spracúvania vykonávaného v mene každého prevádzkovateľa;
c) v príslušných prípadoch prenosy osobných údajov do tretej krajiny alebo medzinárodnej organizácii vrátane označenia predmetnej tretej krajiny alebo medzinárodnej organizácie a v prípade prenosov uvedených v článku 49 ods. 1 druhom pododseku dokumentáciu primeraných záruk;
d) podľa možností všeobecný opis technických a organizačných bezpečnostných opatrení uvedených v článku 32 ods. 1.
[27] Povinné nad 250 zamestnancov.

		Vašej spoločnosti ako prevádzkovateľa? V akých lehotách?	
13.	POSKYTOVANIE SÚČINNOSTI VOČI PREVÁDZKOVATEĽOVI	Je Váš sprostredkovateľ schopný poskytovať nevyhnutnú súčinnosť za účelom dodržiavania a preukázania súladu s požiadavkami Nariadenia? (vedenie záznamov, bezpečnostné opatrenie, oznamovanie incidentov, schopnosť zabezpečiť výkon práv dotknutej osoby, posudzovanie vplyvov, ...)	-
K	**BEZPEČNOSTNÉ OPATRENIA**		
1.		Sú prijaté primerané technické a organizačné opatrenia?	áno
2.		Sú riziká typické pre spracovanie osobných údajov formálne kontrolované, testované a preskúmavané a boli v tomto smere prijaté bezpečnostné opatrenia na zmiernenie identifikovaných rizík a na zabezpečenie celkovej bezpečnosti spracúvania osobných údajov?	áno
3.		Je vypracovaný dokument, ktorý špecifikuje technické, administratívne a fyzické opatrenia na zabezpečenie ochrany osobných údajov? Je aktuálny? V akých intervaloch je aktualizovaný? Kto je zodpovedný za jeho aktualizáciu?	áno Reviduje sa 1-krát ročne podľa potreby ZO
4.		Máte zavedený proces na riešenie sťažností týkajúcich sa bezpečnostných otázok (vo vzťahu k prijatým bezpečnostným opatreniam)?	nie
5.		Je vymenovaná osoba, ktorá je zodpovedná za vypracovanie plánu nápravy a implementáciu nápravy pri identifikácii bezpečnostný dier?	áno
6.		Máte v podmienkach Vašej organizácie inštalované štandardné kryptovacie algoritmy a technológie na prenos, uchovávanie a prijímanie osobných údajov, ktoré sú typické pre odvetvie v ktorom pôsobíte a sú bežne dostupné na trhu?	áno
7.		Sú osobné údaje v podmienkach Vašej organizácie systematicky zničené, vymazané alebo anonymizované, keď už neexistuje potreba ich dlhšie uchovávať? Alebo po splnení účelu, na ktorý boli zozbierané?	áno
8.		Sú prijaté bezpečnostné opatrenia vo forme pseudonymizácie	nie

		osobných údajov vo všetkých oblastiach, kde je pseudonymizácia v podmienkach Vašej organizácie možná?	
9.		Máte prijaté také bezpečnostné opatrenia, ktoré umožňujú prístup a dostupnosť informačných systémov v prípade fyzického alebo technického incidentu (strata dát) a ktoré umožňujú obnoviť napadnuté informačné systémy včas?	áno
L	**KYBERNETICKÁ BEZPEČNOSŤ**		
1.	**POLITIKY**	Máte vypracované bezpečnostné politiky ako napr.: - Informačná bezpečnostná politika - Zásady ochrany osobných údajov - Zásady BYOD - Politika pre riadenia vzdialeného prístupu - Politika pre zabezpečenie siete - Politika používania / prístupu na internet - Emailová a komunikačná politika	áno
2.		Vykonávate pravidelnú kontrolu/previerku prijatých politík? Sú tieto politiky pravidelne aktualizované? V akých intervaloch?	áno
		Je dodržiavanie interných politik kontrolované a ich dodržiavanie vynucované?	Podľa potreby Je kontrolované a čiastočne vynucované doménou
3.		Máte v podmienkach svojej organizácie menovaného člena predstavenstva zodpovedného za kybernetickú bezpečnosť?	nie
4.		Stretáva sa hlavný predstaviteľ informačnej bezpečnosti (IT oddelenie) s členmi predstavenstva zodpovednými za kybernetickú bezpečnosť na pravidelnej báze?	nie
5.		Máte jasne definované zodpovednosti za kybernetickú bezpečnosť s jasnými reportovacími líniami a rozhodovacími procesmi?	nie
6.		Máte zabezpečenú fyzickú ochranu priestorov? Akým spôsobom?	áno

7.		Máte vyčlenený dostatok finančných prostriedkov na zabezpečenie kybernetickej bezpečnosti vo Vašej organizácii?	áno
8.		Sledujete na pravidelnej báze novinky v oblasti kybernetickej bezpečnosti za účelom zabezpečenia aktualizácie kybernetickej bezpečnosti a včasného identifikovania potenciálnych hrozieb?	áno
9.		Máte vypracovaný Reakčný plán postupu pri zisteni bezpečnostných incidentov? Vykonávate pravidelné testovanie a pravidelnú aktualizáciu Reakčného plánu?	nie
		Uzavreli ste primerané poistenie na krytie zodpovednosti v oblasti kybernetickej bezpečnosti?	
10.	ĽUDIA	Máte zavedený mechanizmus na rýchle a efektivne hlásenie podozrivých e-mailov zo strany zamestnancov?	áno
11.		Robíte školenia pre zamestnancov zamerané na oblasť kybernetickej bezpečnosti na pravidelnej báze?	nie
12.		Vykonávate pravidelné previerky zamestnancov, aby ste sa uistili, že rozumejú rizikám počítačovej bezpečnosti? Sú výsledky vyhodnocované a kontrolované, aby sa zabezpečilo kontinuálne zlepšenie?	nie
13.		Majú Vaši zamestnanci vedomosť o rizikách prihlasovania sa do siete internet s firemnými zariadeniami cez verejnú wifi?	áno - IRA
14.		Vykonávate previerky nových zamestnancov ako možné bezpečnostné riziko?	nie
15.	HARDWARE, ÚDAJE, KRYPTOVANIE, TECHNOLÓGIA	Sú ukladané/zálohované dáta šifrované?	nie
16.		Máte implementované vhodné mechanizmy na bezpečné odosielanie súborov?	áno
17.		Máte vypracovaný zoznam serverov a určených jednotlivcov, ktorí sú zodpovední za aktuálnosť tohto zoznamu?	áno
18.		Máte inštalované dostatočný firewall softvér a softvér na	áno

	identifikáciu neoprávneného vstupu/zásahu tretích subjektov?	
19.	Máte zabezpečené testovanie serverov s fiktívnymi dátami (nespôsobilými poškodiť integritu ukladaných dát)?	Odbor IKT
20.	Sú bezdrôtové siete vo Vašej organizácii dostatočne zabezpečené?	áno
21.	Máte softvér na filtrovanie e-mailov a stránok v rámci internetového prehliadania v organizácii?	áno
22.	Kontrolujete pravidelne operačný systém, dáta a software v porovnaní s najnovšími riešeniami dostupnými na trhu za účelom posilňovania kybernetickej bezpečnosti?	áno
23.	Skúmate neúspešné útoky a problémy/neoprávnené zásahy do kybernetickej bezpečnosti a s nimi súvisiace hrozby za účelom prijatia	áno
24.	Máte bezpečnostný plán a pravidelne ho prehodnocujete?	Neviem povedať
	Máte spísaný aktuálny zoznam hardwaru a softwaru?	áno
25.	Máte politiku správy majetku s ohľadom na bezpečnosť?	-
	Máte klasifikované dáta podľa miery ich citlivosti a hroziaceho rizika?	áno
	Máte prijatú vhodnú politiku pre prístup k údajom podľa ich citlivosti a hroziaceho rizika? Limitujete prístup s ohľadom na jednotlivé pracovné pozície?	áno
26.	Máte zabezpečené efektívne šifrovanie dát pri interných prenosoch a pri externých prenosoch?	áno
27.	Zálohujete dáta pravidelne?	áno
	Máte zabezpečenú vhodnú politiku aktualizácie softvérového vybavenia a je používaná dôsledne v podmienkach Vašej organizácie? Ak používate automatický softvér na zabezpečenie aktualizácie, kontrolujete pravidelne jeho funkčnosť a máte o tom k dispozícii nejaké reporty?	áno

28.		Zabezpečujete užívateľom na užívateľských staniciach inštaláciu antivírusového softwaru a jeho aktívnosť po celý čas?	áno
29.		Udržiavate záznam súborov o prihlásení do systému po dobu minimálne jeden rok?	áno
		Používate automatické analyzovanie súborov jednotlivých prihlásení do systému?	nie
		Máte zavedené pravidlá používania externých harddiskov a USB vo Vašej organizácii?	áno
		Vykonávate pravidelné penetračné testy s riadnym vyhodnotením účinnosti prijatých opatrení a analýzou výsledkov?	nie
30.		Využívate prevádzkový monitoring zariadení a aplikácií?	Odbor IKT
31.		Zbierate, archivujete a vyhodnocujete logy zo zariadení a aplikácií? Máte implementovaný Log Management alebo SIEM?	Odbor IKT
32.	**TRETIE STRANY**	Poznáte riziká používania služieb tretích strán v podmienkach Vašej spoločnosti a so zohľadnením nárokov na kybernetickú bezpečnosť?	áno
		Vykonávate previerku tretích strán pred začatím využívania ich služieb?	nie
		Posudzujete tretie strany z pohľadu možného kybernetického rizika?	áno
33.		Máte zabezpečené dostatočne zmluvné povinnosti tretích strán vo vzťahu k zabezpečeniu kybernetickej bezpečnosti a spracúvaných dát?	IRA
34.		Ak používate SaaS alebo cloudové servery máte nastavené zmluvné podmienky tak, aby Váš dodávateľov služieb bol povinný zabezpečiť rýchle informovanie Vašej spoločnosti o potenciálnych bezpečnostných hrozbách?	áno
35.	**VZDIALENÝ PRÍSTUP**	Vyžadujete viacnásobnú autentifikáciu?	áno
		Umožňujete vzdialený prístup? Ak áno, máte dostatočný software na zabezpečenie bezpečnosti?	áno

	Máte dostatočné pravidla pre bezpečnosť mobilných zariadení? Sú dáta v mobilných zariadeniach šifrované?	áno IRA
	Môže byť mobilné zariadenie odstránené na diaľku?	Odbor IKT
	Ak používate BYOD, aplikujete pre bezpečnosť primerané obmedzenia pre osobnú potrebu?	Odbor IKT
	Zvažujete používanie bezpečnostných opatreni na zariadeniach BYOD?	Odbor IKT
36. POUŽÍVATEĽSKÉ KONTÁ / HESLÁ	Vyžadujete samostatné kontá?	áno
	Vyžadujete viacnásobnú autentifikáciu?	áno
	Obmedzujete administrátorské účty na minimum?	áno
	Vyžadujete silné heslá?	áno
	Bránite automaticky používaniu jednoduchých ľahko uhádnuteľných hesiel?	áno

* * *