



ŠKOLIACI MATERIÁL

K WORKSHOPU O GDPR V ONLINE PROSTREDÍ

1. ZÁKLADNÉ INFORMÁCIE

1.1 ZÁKLADNÉ POJMY

- **GDPR** je skratka pre označenie Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov
- **Dotknutá osoba** je fyzická osoba, ktorej osobné údaje sa spracúvajú napr.:
 - zákazník e-shopu
 - osoba, ktorá komunikuje cez kontaktný formulár
 - osoba, ktorej sa zasiela newsletter
 - zamestnanec
 - študent
- **Prevádzkovateľ** je osoba, ktorá určí účel a prostriedky spracúvania osobných údajov, napr.:
 - prevádzkovateľ (vlastník) webovej stránky
 - zamestnávateľ
 - vysoká škola
- **Sprostredkovateľ** je osoba, ktorá spracúva osobné údaje v mene prevádzkovateľa, napr.:
 - poskytovateľ hostingu (pokiaľ zaisťuje uchovávanie osobných údajov, ktoré nie sú šifrované)
 - dopravca zabezpečujúci dodanie tovaru z e-shopu
 - externý mzdový účtovník
- **Informačný systém** na účely ochrany osobných údajov je akýkoľvek usporiadaný súbor osobných údajov. Informačný systém nemusí byť vedený len v elektronickej podobe. Nejedná sa len o softvérové riešenie.
 - databáza osobných údajov obsiahnutých v objednávkach e-shopu
 - databáza kontaktných údajov
 - kniha návštev
 - softvérové riešenie na výpočet poistného

- **Osoba oprávnená spracúvať osobné údaje** je napríklad zamestnanec prevádzkovateľa alebo sprostredkovateľa, ktorý v rámci svojej pracovnej činnosti spracúva osobné údaje.
- **Spracúvanie osobných údajov** je akákoľvek operácia alebo súbor operácií s osobnými údajmi. Spracúvanie môže byť realizované automatizovanými alebo neautomatizovanými prostriedkami, napr.:
 - získavanie
 - zaznamenávanie
 - uchovávanie
 - vymazanie alebo likvidácia

1.2 KDE NÁJDEM INFORMÁCIE O OCHRANE OSOBNÝCH ÚDAJOV?

- **Zákon č. 18/2018 Z.z. o ochrane osobných údajov v znení neskorších predpisov** (účinný od 25.05.2018)
- **Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR)** (účinné od 25.05.2018)
- Metodické usmernenia Úradu na ochranu osobných údajov SR

1.3 SANKCIE ZA NEDODRŽANIE ZÁKONA

- **za porušenie zákona o ochrane osobných údajov hrozí sankcia:**
 - vo výške 10 mil. alebo 2% celosvetového ročného obratu spoločnosti
 - vo výške 20 mil. alebo 4% celosvetového ročného obratu spoločnosti

1.4 AKÚ DOKUMENTÁCIU VYŽADUJE GDPR?

- **súčasťou právnej dokumentácie na ochranu osobných údajov sú:**
 - Posúdenie vplyvu na ochranu osobných údajov, mohol si sa s ním stretnúť aj pod označením DPIA. Nie každý prevádzkovateľ je však povinný vypracovať tento dokument.

To, kedy je jeho spracovanie povinné, vymedzuje priamo GDPR. Ide napríklad o spracúvanie údajov o zdraví vo veľkom rozsahu.

- Záznamy o spracovateľských činnostiach, ktorých vzor nájdeš aj na stránke Úradu na ochranu osobných údajov SR. Zatiaľ čo DPIA bude prijímať menšia časť prevádzkovateľov, vypracovanie záznamov o spracovateľských činnostiach je povinné takmer pre každého.

1.5 AKO POSTUPOVAŤ V PRÍPADE PORUŠENIA OCHRANY OSOBNÝCH ÚDAJOV?

- **porušením bezpečnosti je náhodné alebo nezákonné**
 - Zničenie OÚ
 - Strata OÚ
 - Zmena OÚ
 - Neoprávnené poskytnutie OÚ
 - Neoprávnený prístup k OÚ
- **porušenie môže viesť napríklad k:**
 - diskriminácii
 - krádeži identity
 - zneužitiu identity
 - finančnej strate
 - poškodeniu povesti
 - neoprávnenému zrušeniu pseudonymizácie
- **k porušeniu ochrany môže dôjsť:**
 - zvonka, napr. kybernetický útok
 - zvnútra spoločnosti, napr. neoprávnené sprístupnenie údajov tretej osobe
 - úmyselne
 - z nedbanlivosti
- Už vopred nastav mechanizmus, ktorý odhalí bezpečnostný incident.
- To, že sa včas neodhalí, prevádzkovateľa nijak neospravedlňuje.
- Máš 72 hodín na oznámenie incidentu Úradu na ochranu osobných údajov, prípadne o incidente oboznám svojho nadriadeného.

V určitých prípadoch ti GDPR stanovuje povinnosť informovať aj dotknutú osobu.

- V prípade, ak dôjde k **premeškaniu lehoty 72 hodín**, k oznámeniu je zároveň potrebné pripojiť zdôvodnenie omeškania.
- Ak však bezpečnostný incident nepovedie k riziku pre práva dotknutých osôb (napríklad vďaka Tvojmu dôslednému šifrovaniu), nič oznamovať nemusíš.
- Aké sú prípady z praxe?
 - Zamestnancovi bol ukradnutý služobný notebook, v ktorom boli uložené aj osobné údaje klientov. Notebook bol však šifrovaný a šifrovací kľúč mal k dispozícii len tento zamestnanec a konateľ spoločnosti. Spoločnosť takýto bezpečnostný incident neoznámila Úradu na ochranu osobných údajov SR. – postup je v súlade s GDPR
 - Do online databázy prevádzkovateľa bol zaznamenaný prístup z cudzieho zariadenia. Táto databáza obsahuje údaje o platobných kartách klientov. Prevádzkovateľ oznámil bezpečnostný incident Úradu na ochranu osobných údajov SR. Tento incident však neoznámil dotknutým osobám. – postup nie je v súlade s GDPR

2. PRVÉ KROKY K ZOSÚLADENIU S GDPR

2.2 ČO VŠETKO JE POTREBNÉ POSÚDIŤ PRED ZAČATÍM SPRACÚVANIA OSOBNÝCH ÚDAJOV?

- Právny základ
- Účel spracúvania osobných údajov
- Rozsah osobných údajov
- Dobu spracúvania osobných údajov
- Mechanizmus pre uplatňovanie práv dotknutých osôb
- Poskytovanie osobných údajov tretím subjektom?
- Využívanie služieb sprostredkovateľa?
- Uskutočňovanie prenosu osobných údajov do tretích krajín alebo medzinárodnej organizácii
- Bezpečnostné opatrenia

2.3 AKO ZAISTIŤ SÚLAD S GDPR?

1. **Uskutočniť audit spracúvaných osobných údajov**, pri ktorom preskúmate, kde všade dochádza k spracúvaniu osobných údajov.
2. **Preskúmať, za akým účelom** sa osobné údaje spracúvajú
3. **Minimalizovať rozsah** spracúvaných osobných údajov
4. **Stanoviť lehoty** pre spracúvanie osobných údajov
5. **Preskúmať poskytovanie osobných údajov a prenos do tretích krajín**
6. **Formulovať informácie**, ktoré je potrebné poskytnúť dotknutej osobe pred začatím spracúvania osobných údajov
7. **Upraviť zmluvný vzťah** so sprostredkovateľom
8. Nastaviť postup pre **zabezpečenie výkonu práv dotknutej osoby** a oboznámiť s ním oprávnené osoby
9. Prijatť mechanizmus pre **oznamovanie bezpečnostných incidentov** a oboznámiť s ním oprávnené osoby
10. **Vypracovať bezpečnostnú dokumentáciu** a primerane s ňou oboznámiť oprávnené osoby
11. **Poveriť zodpovednú osobu**, ak prevádzkovateľovi vznikne takáto povinnosť
12. **Poučiť oprávnené osoby**
13. **Prijatť primerané bezpečnostné opatrenia**

2.4 PRÁVNY ZÁKLAD

- **na akom právnom základe budú osobné údaje spracúvané?**
 - Vždy hľadaj dôvod, prečo osobné údaje spracúvaš. Právny základ si predstav ako základňu, o ktorú sa pri spracúvaní osobných údajov musíš opierať. Bez základne predsa nemôžeš začať stavať.
 - Máš 6 možností
 - Dovoľuje ti spracúvanie osobných údajov zákon?
 - Udelila dotknutá osoba súhlas so spracúvaním osobných údajov?
 - Alebo je spracúvanie osobných údajov pre Teba nevyhnutné, pričom by si si bez nich nevedel plniť zmluvné povinnosti?

- Alebo tá k tomu vedie oprávnený záujem?
 - Využiť môžeš taktiež životne dôležité záujmy, či plnenie úlohy vo verejnom záujme.
- Na spracúvanie osobných údajov musí vždy existovať jeden z týchto právnych základov.
- aké právne základy sú najčastejšie využívané v rámci webových stránok a e-shopov?
 - **súhlas so spracúvaním osobných údajov** – napr. pre prihlásenie sa na odoberanie newslettera, členstvo vo vernostnom programe, účasť v spotrebiteľskej súťaži
 - **oprávnený záujem prevádzkovateľa** – napr. kontaktovanie zákazníka e-shopu ohľadom nedokončenej objednávky
 - **spracúvanie osobných údajov je nevyhnutné na účely plnenia zmluvy** – napr. v rámci objednávkového formulára e-shopu

2.5 ÚČEL SPRACÚVANIA

- Spracúvať sa smú len také osobné údaje, ktoré nevyhnutne potrebuješ
- účelom spracúvania osobných údajov vo všeobecnosti môže byť napr. plnenie odvodových povinností zamestnávateľa vo vzťahu k zamestnancovi, plnenie záväzkov vyplývajúcich z uzatvorenej kúpnej zmluvy, a pod.
- **na aké účely môžu byť spracúvané osobné údaje na webovej stránke alebo v e-shope?**
 - poskytovanie zliav a iných výhod členom vernostného programu
 - organizovanie a vyhodnotenie výsledkov spotrebiteľskej súťaže
 - objednávka tovaru alebo služieb v rámci e-shopu
 - zasielanie newslettera a informovanie zákazníka o nových produktoch alebo službách, o zľavách na produkty, o prebiehajúcich alebo plánovaných akciách a pod.

2.6 ROZSAH SPRACÚVANÝCH OSOBNÝCH ÚDAJOV

- ako správne vymedziť rozsah spracúvaných osobných údajov v rámci webovej stránky a e-shopu?

- Zachovaj zásadu minimalizácie osobných údajov
- **na vytvorenie objednávky prostredníctvom objednávkového formulára** – titul, meno, priezvisko, adresa trvalého pobytu alebo prechodného pobytu, resp. adresa pre dodanie tovaru, e-mail, telefón
- **na vedenie vernostného programu** – titul, meno, priezvisko, adresa bydliska, e-mailová adresa, resp. kontaktné údaje a ďalšie údaje relevantné pre vedenie vernostného programu (napr. ak je členstvo vo vernostnom programe podmienené splnením určitých požiadaviek)

2.7 DOBA SPRACOVANIA OSOBNÝCH ÚDAJOV

- Otázkou je, ako dlho chceš (a môžeš) osobné údaje uchovávať? Neustanovuje ti jej dĺžku zákon? Ak áno, musíš sa jej pridržiavať. Za iných okolností smie vyplývať zo súhlasu, prípadne si ju určíš sám. Zamysli sa preto však či je doba spracúvania primeraná?
- **ako správne nastaviť dobu uchovávania osobných údajov získavaných prostredníctvom webovej stránky alebo e-shopu?**
 - doba spracúvania osobných údajov **na účely odoberania newslettera** by mala byť nastavená v súlade s dobou, počas ktorej možno dôvodne predpokladať, že zákazník bude mať záujem o ďalšie služby alebo tovary e-shopu (napr. po dobu 3 rokov)
 - doba spracúvania osobných údajov zadaných do **objednávkového formulára** by mala byť stanovená v súlade s premlčacími lehotami alebo záručnou dobou, v ktorých je zákazník e-shopu (resp. predávajúci) oprávnený uplatňovať nároky vyplývajúce zo zakúpeného tovaru

2.8 ĎALŠIE POVINNOSTI PODĽA GDPR

- Pri novej spracovateľskej operácii je potrebné zabezpečiť aktualizáciu bezpečnostnej dokumentácie. Nezabudni aj na doplnenie záznamu o spracovateľskej činnosti, do úvahy prichádza aj poverenie zodpovednej osoby (ak ešte nebola poverená), či konzultácie s Úradom na ochranu osobných údajov SR

- Ak na web zapracuješ nové funkcionality, premýšľaj, ako by mohli ovplyvniť sféru osobných údajov. Zároveň o tom upovedom „majiteľa“ webu.

2.9 AKÉ SÚ INFORMAČNÉ POVINNOSTI?

- **Pri získavaní osobných údajov je potrebné poskytnúť nasledovné údaje:**
 - Totožnosť a kontakt prevádzkovateľa
 - Kontakt zodpovednej osoby
 - Účel a právny základ spracúvania
 - Prijemcovia
 - Informácia, či sa plánuje prenos osobných údajov
 - Doba uchovávanía
 - Informácie o právach dotknutej osoby
 - Informácia, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou
 - Existencia automatizovaného rozhodovania vrátane profilovania

3. VYMEDZENIE OSOBNÝCH ÚDAJOV

3.1 OSOBNÝ ÚDAJ VŠEOBECNE

- Osobnými údajmi sú všetky informácie, ktoré **identifikujú alebo umožňujú identifikovať** konkrétnu fyzickú osobu.
- Osobné údaje sa týkajú **výlučne fyzickej osoby** (ochrana osobných údajov sa čiastočne vzťahuje na údaje fyzickej osoby podnikateľa)
- Môže ísť o údaje zaznamenané v **grafickej, fotografickej, zvukovej, elektronickej alebo papierovej podobe**
- **V praxi sem možno zahrnúť:** meno, priezvisko, titul, dátum narodenia, číslo občianskeho preukazu, e-mail, údaje o zdravotnom stave, fotografie, záznamy z kamerových zariadení, rodné číslo, lokalizačné údaje, IP adresa, genetické údaje, či biometrické údaje
- Posúdenie či tieto údaje sú osobným údajom **závisí od konkrétnej situácie**, a to najmä:
 - **od kombinácie týchto údajov:**
 - Meno a vek vo svojej kombinácii nie sú osobnými údajmi

- Meno, priezvisko, adresa, dátum narodenia vo svojej kombinácii sú osobnými údajmi
- **od geografického faktoru:**
 - napríklad ak máme informácie o žene, ktorá jazdí na červenom aute v malej obci, je pravdepodobné, že na základe týchto údajov ju niekto identifikuje
 - opačná situácia nastane, ak na základe tých istých údajov budeme hľadať takúto ženu v hlavnom meste. Je veľmi nízka pravdepodobnosť, že ju niekto na základe týchto údajov identifikuje
- Patria sem aj údaje, ktoré poskytujú informácie o **identite fyzickej osoby**, a to o:
 - fyzickej
 - fyziologickej
 - genetickej
 - mentálnej
 - ekonomickej
 - kultúrnej
 - sociálnej identite
- GDPR rozširuje skupinu osobných údajov o tzv. online identifikátory ako sú cookies či IP adresa
- GDPR zároveň rozlišuje tzv. osobitnú kategóriu osobných údajov (napr. údaje o zdraví)

3.2 ČO VŠETKO JE OSOBNÝ ÚDAJ?

- Meno a priezvisko v rámci menšej skupiny ľudí (napr. v podmienkach zamestnávateľa) – áno
- Meno a priezvisko bez územného ohraničenia - skôr nie
- Rodné číslo (bez poznatku o ďalších osobných údajoch a bez prístupu k databáze rodných čísel) – nie
- E-mailová adresa v tvare meno.priezvisko@gmail.com – skôr nie
- E-mailová adresa v tvare meno.priezvisko@zamestnavatel.sk – áno
- Údaje o mzde a iných príjmoch zamestnanca – áno

3.3 SPRACÚVANIE OSOBNÝCH ÚDAJOV

- za spracúvanie osobných údajov je potrebné považovať akékoľvek operácie s týmito údajmi, napríklad:
 - **získavanie** prostredníctvom objednávkového či kontaktného formulára
 - **zaznamenávanie** do elektronickej databázy, do papierového dotazníka
 - **usporadúvanie** podľa roku narodenia
 - **uchovávanie** v rámci softvérových riešení, v mobilných aplikáciách
 - **zmena**
 - **vyhľadávanie** prostredníctvom filtrovania
 - **prehliadanie** v počítačovom programe na vedenie mzdového účtovníctva, v evidencii údajov softvérového riešenia
 - **využívanie**
 - **poskytovanie prenosom** do tretích krajín alebo medzinárodných organizácií
 - **kombinovanie osobných údajov** medzi rôznymi evidenciami, databázami
 - **vymazanie a likvidácia**

3.4 INFORMAČNÝ SYSTÉM

- informačný systém je akýkoľvek **usporiadaný súbor osobných údajov**
- nemusí byť vždy automatizovaný prostredníctvom výpočtovej techniky, môže byť vedený v listinnej ako aj elektronickej podobe, či kombinovane
- **príklady informačných systémov:**
 - IS Personalistika a mzdy
 - IS Zmluvná agenda
 - IS Účtovné doklady
 - **IS E-shop**
 - **IS Webová stránka**
 - **IS Spotrebiteľská súťaž**
 - **IS Vernostný program**

- **IS Reklamácie**
- nejedná sa teda o informačný systém v zmysle „aplikácia“, „softvér“ či „databáza na serveri“
- informačným systémom môže byť aj **kartotéka, kniha návštev a pod.**

4. SÚHLAS

4.1 SÚHLAS SO SPRACÚVANÍM OSOBNÝCH ÚDAJOV

- **Súhlas by mal byť získaný tak, aby si bol schopný preukázať jeho udelenie. Písomná forma sa nevyžaduje, ale ...** ústne udelenie súhlasu je v poriadku, pokiaľ si schopný preukázať jeho udelenie (napr. formou audionahrávky)
- udelenie súhlasu elektronicky je možné preukázať zaznamenávaním **logov či príznakov v databáze**
- ...
- **Zo súhlasu by malo byť zrejmé:**
 - kto súhlas udelil
 - ako bol súhlas udelený
 - kedy ho udelil
 - o čom všetkom bola osoba pred udelením súhlasu informovaná
 - údaj o tom, či bol súhlas odvolaný
- súhlas nemusí byť udelený **písomne, avšak táto forma je najvhodnejšia**
- súhlas so spracúvaním osobných údajov by **nemal byť podmienený súhlasom s inými podmienkami** (napr. VOP)
- súhlas by mal byť formulovaný **jednoducho a zrozumiteľne** – tak, aby informáciám každý porozumel
- pred udelením súhlasu je potrebné poskytnúť **informácie, ktoré stanovuje GDPR**
- dotknutá osoba je oprávnená svoj súhlas **kedykoľvek odvolať**
- súhlas by mal byť udelený **aktívnym konaním dotknutej osoby** (napr. nie je prípustné, aby na webovej stránke bolo vopred zaškrtnuté políčko pre udelenie súhlasu)

- **je určenie doby, na ktorú sa súhlas udeľuje v súlade s GDPR?**
 - na 3,6,11,... rokov od udelenia súhlasu – áno
 - na dobu neurčitú - nie
 - po dobu trvania pracovného pomeru - áno
 - do doby odvolania súhlasu - nie
 - bez uvedenia doby - nie
- **v súhlase by malo byť vymedzené:**
 - osobné údaje, ktorých sa súhlas týka
 - účel spracúvania
 - doba spracúvania
 - vyhlásenie, že dotknutej osobe boli poskytnuté zákonom stanovené informácie vrátane poučenia o jej právach
 - vyhlásenie, že dotknutá osoba bola poučená o možnosti kedykoľvek odvolať svoj súhlas
- **Predtým ako sa rozhodneš spracúvať osobné údaje na základe súhlasu, vylúč všetky ostatné možnosti. Dôvodov je niekoľko:**
 - súhlas je ľahko odvolateľný
 - súhlas nie je jednoduché získať
 - udelenie súhlasu nie je jednoduché hodnoverne preukázať
 - získanie súhlasu môže byť vyhodnotenú ako neslobodnú

4.2 ZÁKLADNÉ PODMIENKY PRED UDDELENIE SÚHLASU

1. Pred spracúvaním osobných údajov na základe súhlasu dotknutej osoby si over že nie je možné využiť iný právny základ (napr. oprávnený záujem).
2. Preskúmaj, či žiadosť o udelenie súhlasu spĺňa stanovené podmienky
 - A. je ľahko odlíšiteľná od iných častí dokumentu (prípadne webovej stránky)
 - B. nie je súčasťou všeobecných obchodných podmienok
 - C. nie je súčasťou iných formulárov (napr. formulárových zmlúv)
3. Žiadosť o udelenie súhlasu ako aj súhlas samotný je formulovaný jasne a zrozumiteľne.

4. Subjekty majú možnosť zaškrtnúť udelenie súhlasu, to znamená, že udelenie súhlasu nie je preddefinované (využíva sa opt-in namiesto opt-out). Nevyužívajú sa vopred zaškrtnuté políčka.
5. Pred udelením súhlasu sú poskytované základné informácie o účeloch získavania súhlasu a ďalšie informácie uvedené v čl. 13 GDPR (plnenie informačnej povinnosti zahŕňa napr. informácie o totožnosti).
6. žiadosť o udelenie súhlasu je formulovaná tak, aby bolo možné vyjadriť súhlas len s vybranými spracovateľskými operáciami, resp. s vybranými účelmi spracúvania.
7. Pred udelením súhlasu sú dotknutej osobe poskytované informácie o tom, akým spôsobom je možné súhlas odvolať.
8. V prípade, ak nedôjde k udeleniu súhlasu so spracúvaním osobných údajov, nie sú s takouto situáciou spájané žiadne negatívne následky.
9. Udelenie súhlasu nie je podmienkou poskytovania služieb, resp. čerpania iných výhod, zliav a pod.
10. Dôležitá je aj interná evidencia o podmienkach udelenia súhlasu (napr. akým spôsobom bol súhlas udelený, doba spracúvania, kedy bol súhlas udelený a pod.), ako i internú evidenciu o tom, k čomu konkrétny subjekt udelil súhlas so spracúvaním osobných údajov.

5. SUBJEKTY OCHRANY OÚ

5.1 KOHO SA TÝKA OCHRANA OSOBNÝCH ÚDAJOV?

- chránené sú **všetky osobné údaje fyzických osôb** (za určitých okolností podliehajú ochrane aj údaje týkajúce sa fyzickej osoby podnikateľa, či určených osôb konajúcich v mene právnickej osoby)
- **povinnosti stanovené v GDPR sa týkajú všetkých, ktorí spracúvajú osobné údaje pre inú ako osobnú alebo domácu potrebu, napr.**
 - zamestnávateľov
 - miest a obcí
 - škôl
 - nemocníc
 - prevádzkovateľov e-shopov
 - prevádzkovateľov webových stránok
 - prevádzkovateľov kamerových systémov

5.2 VYUŽÍVANIE SLUŽIEB SPROSTREDKOVATEĽA

- **sprostredkovateľ spracúva osobné údaje v mene prevádzkovateľa**
- ak by si si napríklad v budúcnosti založil vlastnú firmu a účtovníctvo by mal na starosti externý mzdový účtovník, vystupoval by voči tvojej firme ako sprostredkovateľ. Prečo? Prichádzal by do kontaktu s osobnými údajmi tvojich zamestnancov, či klientov, a to v mene tvojej firmy
- medzi prevádzkovateľom a sprostredkovateľom musí byť uzatvorená **zmluva o spracúvaní osobných údajov**
- Dbaj na výber správneho a spoľahlivého sprostredkovateľa, ten by mal totiž spĺňať požiadavky na technické a organizačné opatrenia
- **v prípade, že pri novej spracovateľskej operácii budete využívať služby sprostredkovateľa:**
 - vyberte sprostredkovateľa, ktorý poskytuje dostatočné záruky
 - preverte jeho technickú a organizačnú pripravenosť (napr. prostredníctvom dotazníka)
 - uzatvorte zmluvu o spracúvaní osobných údajov
 - zabezpečte kontrolu dodržiavania povinností
- **sprostredkovateľom v rámci služieb webovej stránky a e-shopu môžu byť nasledovné subjekty:**
 - poskytovateľ šablóny e-shopu (nízka pravdepodobnosť)
 - poskytovateľ webhostingu
 - doručovatelia tovaru z e-shopu
 - posúdenie postavenia tretích subjektov, ktoré sa podieľajú na poskytovaní služieb webovej stránky alebo e-shopu závisí od konkrétnych okolností

5.3 PRÁVA DOTKNUTEJ OSOBY

- **Medzi práva dotknutej osoby patria:**
 - Právo na opravu
 - Právo na „zabudnutie“
 - Právo na prenosnosť
 - Právo na prístup k údajom
 - Právo namietat'
 - Právo namietat' proti priamemu marketingu

- Právo podať sťažnosť
- Právo na súdnu ochranu
- Právo na náhradu škody a nemajetkovej ujmy
- Právo podať oznámenie o skutočnostiach nasvedčujúcich, že bol spáchaný trestný čin

5.4 ČO V PRÍPADE, AK DOTKNUTÁ OSOBA UPLATNÍ SVOJE PRÁVA?

Všeobecný postup by mohol vyzerat' nasledovne:

- Dotknutá osoba si uplatní právo poslaním žiadosti – väčšinou emailom, prípadne poštou
- Preskúmaj, či je sa jedná o dotknutú osobu, ktorej údaje sa spracúvajú – nezabudni na preskúmanie totožnosti. Práva môže uplatniť len osoba, ktorej sa osobné údaje týkajú.
- následne, posúď či sú splnené podmienky GDPR pre uplatnenie tohto práva
- Ak žiadosť nespĺňa podmienky pre uplatnenie práva, informuj dotknutú osobu o dôvodoch nevyhovenia žiadosti a o možnosti podať sťažnosť Úradu na ochranu osobných údajov SR
- Nezabúdaj, že aj vybavenie žiadosti dotknutej osoby podlieha stanoveným lehotám.

5.5 UPLATŇOVANIE PRÁV DOTKNUTÝCH OSÔB

- Pred začatím spracúvania osobných údajov si nastav mechanizmus pre uplatňovanie práv dotknutých osôb
- v prípade, ak sa rozhodneš osobné údaje získané prostredníctvom webovej stránky uchovávať v osobitných databázach, je potrebné pri uplatnení práva dotknutej osoby zaistiť súčinnosť medzi tebou, t.j. osobou, ktorá dbá na správne fungovanie webovej stránky a „majiteľom“ webovej stránky, ktorý je zároveň prevádzkovateľom osobných údajov
- v rámci webovej stránky je potrebné:
 - poskytovať informácie o postupe, akým môže dotknutá osoba uplatniť svoje práva
 - poskytovať kontaktné údaje, prostredníctvom ktorých môže dotknutá osoba uplatňovať svoje práva

- poskytovať kontaktné údaje na zodpovednú osobu, ak došlo k jej povereniu

5.6 KTO JE ZODPOVEDNÁ OSOBA?

- **Zodpovedná osoba vykonáva dohľad nad dodržiavaním GDPR**
- Vo firme by dohliada na to, aby všetky operácie, pri ktorých sa spracúvajú osobné údaje, boli vždy vykonávané s náležitým rešpektom k súkromiu jednotlivcov a boli v súlade s GDPR.
- Zodpovednú osobu však nemusí mať ustanovenú každá jedna firma
- v prípade, že bola vo vašej spoločnosti ustanovená zodpovedná osoba, odporúčame **konzultovať s ňou otázky týkajúce sa spracúvania osobných údajov**

6. WEBY A E-SHOPY

6.1 OSOBNÝ ÚDAJ NA WEBOVEJ STRÁNKE A E-SHOPE

- Prostredníctvom webovej stránky môžu byť spracúvané nasledovné osobné údaje:
 - osobné údaje obsiahnuté v kontaktnom formulári: meno, priezvisko, telefón, e-mail, korešpondenčná adresa, ako aj osobné údaje, ktoré môžu byť obsiahnuté v tele doručovanej správy
 - osobné údaje získavané na účely zasielania newslettera: e-mailová adresa
 - osobné údaje získavané na účely využívania nástrojov e-shopu ako napr. opustený košík, upselling, segmentácia: informácie o predchádzajúcich nákupoch, o správaní používateľa na webovej stránke, o jeho preferenciách tovaru a služieb
- Je e-mail osobným údajom?
 - samotný e-mail, ktorý nie je v kombinácii s inými údajmi (ako napríklad, dátum narodenia, adresa trvalého pobytu a pod.) môže byť osobným údajom
 - e-mail, ktorý nie je osobným údajom: slniecko123@gmail.com
 - e-mail, ktorý je osobným údajom: albert.novy@positive.sk

- e-mailová adresa, ktorá poskytuje údaje o mene, priezvisku a zamestnávateľovi alebo inej príslušnosti k organizačnej štruktúre bude zväčša osobným údajom (aj bez kombinácie s inými údajmi)

6.2 AKO ZAISTIŤ SÚLAD WEBOVEJ STRÁNKY A E-SHOPU S GDPR?

Pri spracúvaní osobných údajov prostredníctvom webovej stránky a e-shopu je potrebné GDPR zohľadniť v nasledovných častiach:

- kontaktný formulár
- odoberanie newslettera
- cookies
- objednávkový formulár
- online marketing (priamy marketing a behaviorálna reklama)
- vernostný program
- ponuka produktov e-shopu osobe mladšej ako 16 rokov
- wishlist
- narodeninové prania pre zákazníka
- opustený košík
- poskytnutie zliav pre opätovnú návštevu e-shopu
- prehľad o nákupoch zákazníka a zacielenie newslettera (segmentácia)
- upselling
- zaistenie webhostingu
- výkon primeraných bezpečnostných opatrení
- poskytovanie technickej podpory
- využívanie krabicových riešení e-shopu
- porušenie ochrany osobných údajov