**2. Tabulková část (soubor 02\_GDPR\_v\_ordinaci\_tabulkova\_cast.xlsx)**

**Výklad**

Při čtení tohoto výkladu si vezměte k ruce vždy příslušnou tabulku a sledujte její obsah současně s výkladem. Lépe pak výkladu porozumíte.

**O co tady jde?**

Je to jednoduché:

1. v tabulce č. 1 si uděláte přehled všeho, co s osobními údaji ve své ordinaci děláte (nebojte se, většinu záznamů jsme Vám už připravili),
2. v tabulce č. 2 si řeknete, zda jsou u Vás osobní data nějak ohrožena a co by se případně mohlo stát, pokud by nějaká hrozba skutečně nastala (i to jsme z velké většiny udělali za Vás),
3. tabulka č. 3 vyhodnotí rizikovost zpracování osobních údajů (tady je to úplně snadné: tabulka to udělá sama – a barevně 😊)
   1. **Tabulka č. 1 – Záznamy o činnostech zpracování**

Záznamy o činnostech zpracování jsou povinnou dokumentací, kterou musí mít každý správce osobních údajů. Jde vlastně o přehled všech kategorií osobních údajů, které správce zpracovává, a způsobů jejich zpracování. Správce, který má Záznamy o činnostech zpracování, si udělá jasno o tom,

* které osobní údaje zpracovává (např. jméno, příjmení, rodné číslo, údaje o zdravotním stavu),
* jak a kde je zpracovává (např. ve zdravotnické dokumentaci),
* zda má pro zpracování nějaké oprávnění, tzv. titul (např. mu zpracování ukládá zákon, nebo smlouva s pacientem apod.),
* za jakým účelem osobní údaje zpracovává.

Tabulce č. 1 věnujte prosím velkou pozornost. Jde o klíčový dokument, jehož obsah musí odpovídat poměrům ve Vaší ordinaci. Jde vlastně o strukturovaný popis všeho, co se nějak dotýká osobních údajů zpracovávaných ve Vaší ordinaci. Další části materiálu „*GDPR v ordinaci zubního lékaře*“ vycházejí z tabulky č. 1, a proto je opravdu důležité, aby tabulka č. 1 odpovídala realitě.

Tabulka č. 1 je již částečně vyplněna. Obsahuje zpracování osobních údajů, k nimž obvykle dochází v ambulanci zubního lékaře. Aby se z tabulky č. 1 staly Vaše skutečné záznamy o činnostech zpracování, musíte ji doplnit:

* ve žluté části vyplňte údaje o správci (tedy o sobě, pokud poskytujete zdravotní služby vlastním jménem, nebo o právnické osobě, která je poskytovatelem). Řádky *„pověřenec pro ochranu osobních údajů“* a *„posouzení vlivu zpracování na ochranu osobních údajů“* nevyplňujte. Pověřence pro ochranu osobních údajů totiž nebudete jmenovat a posouzení vlivu zpracování na ochranu osobních údajů nebudete provádět, protože Vám to GDPR neukládá. Vysvětlení, proč tomu tak je, najdete v části Právní rozbory. (opakované upozornění: tento materiál je určen jen pro jednotlivé poskytovatele s méně než 10 ošetřujícími zdravotnickými pracovníky. Pokud tuto podmínku nesplňujete, materiál nepoužívejte.)
* v bílé části jsou uvedena obvyklá zpracování osobních údajů, k nimž dochází v běžné ordinaci zubního lékaře. I zde může být potřeba text přizpůsobit poměrům ve Vaší ordinaci. Často bude např. třeba upravit formu zpracování (pokud např. vedete zdravotnickou dokumentaci jen v listinné formě, bude třeba odpovídajícím způsobem upravit položku *„forma zpracování“*).

Pokud se některý zdroj osobních údajů ve Vaší ordinaci nevyskytuje (např. neobjednáváte pacienty, a proto nemáte objednací knihu), je třeba odpovídající řádek z tabulky č. 1 odstranit (upozornění: odstraníte-li řádek z tabulky č. 1, je třeba odpovídající řádek odstranit též z tabulek č. 2 a č. 3).

Provádíte-li nějaké další zpracování osobních údajů, je třeba je do bílé části tabulky č. 1 doplnit. K tomu Vám může posloužit tabulka č. 4 – Příklady dalších zpracování osobních údajů. Zde jsou uvedeny jednak příklady zpracování, která se v praxi vyskytují méně často, a jednak obecná charakteristika obsahu jednotlivých položek tabulky č. 1 – Záznamů o činnostech zpracování.

Pokud v tabulce č. 4 najdete zpracování, které provádíte, prostě příslušný řádek zkopírujte na volné místo bílé části tabulky č. 1.

Není možné popsat všechny možné zdroje osobních údajů a všechny možné účely zpracování. Pokud tedy provádíte zpracování, které není uvedeno ani v tabulce č. 1, ani v tabulce č. 4, musíte sami příslušný záznam v bílé části tabulky č. 1 vytvořit. Postupujte analogicky podle záznamů, které jsme v tabulkách již předepsali, a podle obecných charakteristik uvedených v posledním řádku tabulky č. 4.

* 1. **Tabulka č. 2 –** **obvyklá rizika pro práva a svobody subjektů údajů**

Každý správce osobních údajů musí v určité míře zhodnotit, jaká rizika přináší zpracování osobních údajů, které provádí, pro práva a svobody. Jednotlivý poskytovatel, u kterého pracuje méně než 10 zdravotnických pracovníků, může provést jen základní zhodnocení a není povinen provádět složitější posouzení vlivu na ochranu osobních údajů (proč tomu tak je, vysvětluje právní rozbor této otázky, který je součástí dokumentace pod bodem 6). Tabulka č. 2 je povinnou součástí dokumentace správce osobních údajů.

Ve žluté části tabulky č. 2 najdete:

* v prvním sloupci zdroje údajů. Údaje se přepisují automaticky z tabulky č. 1, do prvního sloupce tabulky č. 2 proto není třeba nic dopisovat.
* ve druhém sloupci hrozby. Jde o standardní obecně uznávanou klasifikaci toho, co se s osobními údaji může stát:
* narušení důvěrnosti znamená, že se s údaji seznámil někdo, kdo k tomu neměl oprávnění;
* narušení integrity znamená, že údaje byly pozměněny či upraveny;
* narušení dostupnosti znamená, že údaje sice existují, nelze je ale použít (např. poškozený počítač, odcizená karta pacienta);
* ztráta údajů znamená, že údaje byly nenávratně ztraceny (smazaný pevný disk počítače, požár apod.).

Do druhého sloupce tabulky č. 2 rovněž není třeba nic dopisovat.

* ve třetím sloupci zhodnocení míry pravděpodobnosti, s jakou příslušná hrozba může ve vztahu k příslušnému zdroji informací nastat. Zhodnocení je provedeno na stupnici 1 až 5, kde 1 znamená nejnižší pravděpodobnost a 5 nejvyšší pravděpodobnost.

*Příklad:*

*Hodnota 1 v řádku „narušení integrity osobních údajů“ u položky „zdravotnická dokumentace“ znamená, že je velmi nízké riziko, že dojde k pozměnění údajů ve zdravotnické dokumentaci. Proč tomu tak je? Protože změny ve zdravotnické dokumentaci musí každý poskytovatel podle zákona provádět výlučně tak, aby byl patrný stav před provedenou změnou. Zdravotnická dokumentace je umístěna trvale v ordinaci, přístup k ní mají jen oprávněné a poučené osoby. Není proto důvod se obávat, že by došlo k narušení její integrity.*

*Příklad:*

*Hodnota 4 v řádku „narušení důvěrnosti údajů“ u položky „adresáře pacientů (včetně systematicky uspořádaných vizitek pacientů“ vyjadřuje relativně vysoké riziko, že se někdo neoprávněný seznámí s údaji z adresáře. Proč? Adresář či vizitky jsou uloženy na stole pro rychlé použití, nahlédnout do nich může uklízečka po ordinační době nebo náhodou i některý pacient, který přichází do ordinace.*

Hodnoty, které jsme předepsali do třetího sloupce tabulky 2, vycházejí z toho, že Vaše ordinace splňuje minimální zákonné předpoklady, uvedené v dokumentaci v části 3 – popis modelové ordinace (minimální standardy zabezpečení osobních údajů). Pokud byste některý předpoklad nesplňovali, je třeba hodnoty rizika přiměřeně zvýšit.

*Příklad:*

*Jedním z minimálních předpokladů je, že karta po vyjmutí z kartotéky je přístupná jen zdravotnickým pracovníkům, kteří poskytují dotčenému pacientovi zdravotní služby. I proto je v tabulce č. 2 hodnoceno riziko narušení důvěrnosti zdravotnické dokumentace jako relativně nízké (hodnota 2). Jestliže ale ve Vaší ordinaci sestra ráno připraví karty objednaných pacientů a položí je volně v čekárně na stůl, je zřejmé, že riziko, že se některý pacient do těchto karet podívá, je velmi vysoké (hodnota by v takovém případě musela být nejméně 4, spíše 5).*

V modré části tabulky č. 2 jsou nejdůležitější práva a svobody, která mohou být zpracováním osobních údajů dotčena. Čísla v modré části tabulky č. 2 představují význam konkrétního práva na stupnici 1 až 5. Obsah modré části jsme vytvořili na základě odborné právní úvahy a není třeba jej měnit.

Čísla v bílé části tabulky představují zhodnocení závažnosti dopadu konkrétní realizované hrozby do konkrétního práva subjektu údajů na stupnici 1 až 5.

*Příklad:*

*Hodnota 5 v řádku „narušení důvěrnosti osobních údajů“ u položky „zdravotnická dokumentace“ ve sloupci „právo na soukromí“ znamená, že pokud se někdo neoprávněný dozví údaje o zdravotním stavu pacienta ze zdravotnické dokumentace, bude to mít zcela zásadní dopad do jeho soukromí. Ve stejném řádku je ve sloupci „právo na život“ hodnota 1. To znamená, že únik informací ze zdravotnické dokumentace bude zpravidla znamenat velký zásah do soukromí pacienta, ale na životě jej to neohrozí. Pokud by se ale údaje ze zdravotnické dokumentace ztratily nebo byly pozměněny, zásah do práva na život může být závažnější: v důsledku chybějících údajů může být podán nesprávný lék apod. Proto jsou hodnoty v řádku „narušení integrity“ či „ztráta“ ve sloupci „právo na život“ významně vyšší (hodnota 3).*

Čísla v bílé části tabulky jsme vytvořili na základě odborné úvahy a není třeba je měnit. Pokud ale do tabulky č. 1 doplníte nějaké nové zpracování, automaticky se překopíruje do prvního sloupce tabulky č. 2. V takovém případě budete muset sami vyhodnotit jak pravděpodobnost hrozby ve žluté části, tak závažnost dopadu hrozby v bílé části tabulky č. 2.

Upozornění: pokud z tabulky č. 1 odstraníte některý řádek (protože obsahuje zpracování, které neprovádíte), odstraňte prosím odpovídající řádek i z tabulky č. 2 a č. 3.

* 1. **Tabulka č. 3 – základní zhodnocení obvyklých rizik**

Tabulka č. 3 funguje zcela automaticky, není třeba do ní nic doplňovat. Přebírá údaje z tabulky č. 1 a tabulky č. 2 a vyhodnocuje je. Čísla představují číselné zhodnocení míry rizika na stupnici od 0 do 125. Čím je číslo vyšší, tím je míra rizika zpracování pro práva a svobody vyšší. Tabulka míru rizika vyjadřuje i barevně.

Obecně lze říci, že hodnota vyšší než 50 je nepřijatelná. Pokud u některého zpracování takové hodnoty dosáhnete, je třeba buď takové zpracování ukončit, anebo přijmout některé technicko-organizační opatření ke snížení rizika.

*Příklad:*

*Tabulka č. 3 tak, jak jsme ji pro Vás připravili, neobsahuje žádné nepřijatelné riziko. Je tomu tak proto, že zhodnocení předpokládá, že Vaše ordinace splňuje základní standardy zabezpečení vyplývající z platných právních předpisů a neprovádí žádná riziková zpracování.*

*Jedním ze způsobů zpracování osobních údajů, které není typické, ale v praxi se vyskytuje, je zasílání údajů o zdravotním stavu (např. výsledky vyšetření apod.) pacientům nebo kolegům e-mailem. Protože nejde o typické zpracování, není uvedeno v tabulce č. 1, ale jako příklad je uvedeno v tabulce č. 4 a jeho zhodnocení je jako příklad uvedeno v tabulce č. 5 (v tabulkách jsou příslušné řádky zvýrazněny červeně). Pokud byste popis takového zpracování zkopírovali z tabulky č. 4 do tabulky č. 1 a jeho zhodnocení z tabulky č. 5 do tabulky č. 2, zjistili byste v tabulce č. 3, že jde o zpracování s nepřijatelnou, a tedy nepřípustnou mírou rizika. Takové zpracování nelze provádět, a to ani se souhlasem pacienta. Co s tím? Buď přestanete pacientům sdělovat e-mailem informace o zdravotním stavu, anebo zavedete se svými pacienty šifrovanou komunikaci. Pak budete moci v tabulce č. 2 významně snížit zhodnocení pravděpodobnosti, že dojde k narušení důvěrnosti e-mailových zpráv (ze stávajících 5 na 1 až 2). Tím dojde i ke snížení celkové míry rizika tohoto zpracování na přijatelnou hodnotu.*

*Jiná je ale situace, pokud se svými pacienty komunikujete e-mailem, avšak nikoliv o jejich zdravotním stavu (např. po e-mailu pacienty objednáváte). Takové zpracování je rovněž jako příklad uvedeno v tabulce č. 4 (řádek 8) a vyhodnoceno v tabulce č. 5. Pravděpodobnost, že si e-mailovou komunikaci přečte někdo nepovolaný, je zde stále vysoká. Dopady do práv pacientů jsou však nižší: pokud se někdo cizí dozví, že je k Vám konkrétní pacient objednán, není to sice správné, avšak není to zdaleka takový problém, jako kdyby získal přístup k laboratorním výsledkům předoperačního vyšetření. E-mailová komunikace, pokud neobsahuje údaje o zdravotním stavu, tak bude podstatně méně riziková, a tudíž přípustná.*

Upozornění: pokud z tabulky č. 1 odstraníte některý řádek (protože obsahuje zpracování, které neprovádíte), odstraňte prosím odpovídající řádek i z tabulky č. 2 a č. 3.

* 1. **Tabulka č. 4 – příklady dalších zpracování osobních údajů**

Tabulka č. 4 obsahuje příklady některých méně obvyklých zpracování osobních údajů. Není součástí povinné dokumentace správce osobních údajů. Jde jen o pomůcku, kterou můžete využít při individualizaci tabulky č. 1 – Záznamy o činnostech zpracování.

* 1. **Tabulka č. 5 – příklady základního zhodnocení dalších rizik**

Tabulka č. 5 obsahuje příklady zhodnocení rizik méně obvyklých zpracování osobních údajů, která jsou uvedena v tabulce č. 4. Není součástí povinné dokumentace správce osobních údajů. Jde jen o pomůcku, kterou můžete využít při individualizaci tabulky č. 2 – Rizika pro práva a svobody subjektů údajů.