Univerzita Pardubice

Fakulta ekonomicko-správní

Vliv GDPR na oblast e-commerce

Klára Konečná

Bakalářská práce

2019

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Klára Konečná**

Osobní číslo: **E16212**

Studijní program: **B6208 Ekonomika a management**

Studijní obor: **Ekonomika a provoz podniku**

Název tématu: **Vliv GDPR na oblast e-commerce**

Zadávající katedra: **Ústav podnikové ekonomiky a managementu**

Zásady pro vypracování:

Cílem práce je ozřejmit pojem GDPR a posoudit jeho vliv na oblast e-commerce. Součástí práce je zpracování návodu, jak připravit e-shop nebo webovou prezentaci v souladu s pravidly GDPR.

Osnova:

— Představení a důvody k zavedení GDPR

— Změny v elektronickém obchodování v důsledku nové legislativy

— Návod na zpracování e-shopu v souladu s pravidly GDPR

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

JANOUCH, Viktor. Internetový marketing. 2. vyd. V Brně: Computer Press, 2014. ISBN 978-80-251-4311-7.
MIKULÁŠKOVÁ, Petra a Mirek SEDLÁK. Jak vytvořit úspěšný a výdělečný internetový obchod. Brno: Computer Press, 2015. ISBN 978-80-251-4383-4.
SEDLÁČEK, Jiří. E-komerce, internetový a mobil marketing. Praha: BEN - technická literatura, 2006. ISBN 80-7300-195-0.
ŽŮREK, Jiří. Praktický průvodce GDPR: včetně úplného znění GDPR. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9.

Vedoucí bakalářské práce: **Ing. Renáta Bílková, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **3. září 2018**

Termín odevzdání bakalářské práce: **30. dubna 2019**

doc. Ing. Romana Provazníková, Ph.D.
děkanka

L.S.

doc. Ing. Marcela Kožená, Ph.D.
vedoucí ústavu

V Pardubicích dne 3. září 2018

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byl/a jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47 b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 18.4.2019

Klára Konečná

PODĚKOVÁNÍ

Na tomto místě bych ráda poděkovala své vedoucí práce Ing. Renátě Bílkové, PhD., a to nejen za odborné rady a vedení, ale i za její lidský přístup, zejména trpělivost a vstřícnost, které mi prokazovala od první chvíle až do odevzdání této práce.

ANOTACE

Bakalářská práce se zabývá vlivem Obecného nařízení o ochraně osobních údajů na oblast e-commerce. V první části práce jsou popsané a vysvětlené důležité pojmy a definice z tohoto evropského právního předpisu, následované popisem jeho vlivu na jednotlivé oblasti a procesy elektronických obchodů. V závěru této práce je na základě těchto teoretických poznatků vytvořen grafický návod pro zpracování e-shopu v souladu s GDPR.

KLÍČOVÁ SLOVA

e-commerce, e-business, elektronický obchod, GDPR, osobní údaje

TITLE

GDPR and its impact on e-commerce

ANNOTATION

The thesis deals with the influence of the General Data Protection Regulation on e-commerce. The first part describes and explains important terms and definitions of this European regulation, followed by the description of its impact on individual areas and processes of e-shops. At the end of this work are, based on the theoretical knowledge, created graphic instructions for designing an e-shop in accordance with GDPR.

KEYWORDS

e-commerce, e-business, e-shop, GDPR, personal data

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

B2B	Business to business
B2C	Business to customer
ČIA	Český institut pro akreditaci
GDPR	Obecné nařízení o ochraně osobních údajů
MPSV	Ministerstvo práce a sociálních věcí
MVČR	Ministerstvo vnitra České republiky
ÚOOÚ	Úřad pro ochranu osobních údajů
VOP	Všeobecné obchodní podmínky
ZOOÚ	Zákon o ochraně osobních údajů

Úvod

E-commerce, neboli elektronický obchod, je stále se rozšiřujícím fenoménem posledních desetiletí a za tu dobu se stal neoddělitelnou součástí našich životů. Je umožněný nástupem internetu, který zároveň smazal hranice mezi jednotlivými státy a míra globalizace z velké části znemožnila ochranu spotřebitelů národními právními předpisy. Z toho důvodu je nutné regulovat toto prostředí na nadnárodním měřítku a co možná nejvíce jednotně.

V této bakalářské práci bude popsán vliv Obecného nařízení o ochraně osobních údajů (neboli GDPR) Evroské Unie, jehož účelem je právě taková regulace aspirující na zvýšení ochrany evropských občanů v oblasti zacházení s osobními údaji (nutno dodat, že jeho dopady jsou skutečně dalekosáhlé a změny postihly v podstatě všechna odvětví podnikání, nejen elektronický obchod).

Cílem této práce je ozřejmit pojem GDPR a následně popsat nejdůležitější oblasti a způsoby jeho vlivu na e-commerce a následně vytvořit návod na připravení e-shopu tak, aby byl v souladu s pravidly GDPR.

Nejprve je nastíněn samotný účel a stručně i historický vývoj ochrany osobních údajů, následně jsou popsané vybrané pojmy, působnost a zásady Obecného nařízení. Poté následuje část mapující změny, které v provozování e-shopu nastaly se vstupem GDPR v platnost a poslední kapitolou je návod, jak zpracovat e-shop. Návod je zpracován i v grafické formě, která tvoří přílohu této bakalářské práce.

1 HISTORICKÝ VÝVOJ OCHRANY OSOBNÍCH ÚDAJŮ

Pro mladou generaci je těžko představitelný stav, ve kterém se osobní údaje nevyskytují v ohromném měřítku a **nepotřebují** ochranu. Již několik desítek let rozsah zpracovávaných informací setrvale roste, a i když současná společnost často vyjadřuje opovržení nad socialistickým způsobem vytváření „složek" a na obyvatele, teď existuje mnohem více záznamů nejen o chování člověka, ale také o jeho zálibách, o tom, co se mu líbí a nelíbí, a v neposlední řadě posuzování, zda je vhodným kandidátem k té či oné službě (např. **profilování** žadatelů o úvěr).

Jako okamžik vyčlenění zvláštní části práva na ochranu soukromí by se dala označit *Úmluva o ochraně osob s ohledem na automatizované zpracování osobních údajů*, která je zároveň **první nadzákonný právní instrument** v této oblasti. Tento dokument byl vytvořen členskými státy Rady Evropy, které ho podepsaly jako *Úmluvu Rady Evropy č. 108* a ta vstoupila v platnost dne 28. ledna 1981 (ÚOOÚ, 2018a). Jménem České Republiky byla podepsána v roce 2000 a nabyla platnosti dne 1. listopadu 2001 (MVČR, 2001).

Během téměř dvacetiletého období od doby, kdy se státy Rady Evropy zavázaly k dodržování Úmluvy a datem 1.6.2000, bylo v **českém právu** alternativní ustanovení zakotveno pouze v *Listině základních práv a svobod*. Ta je účinná od 1.1.1993 a osobním údajům se v ní nepřímo věnuje článek 7 (1) a článek 10 (1), (2) a zejména (3):

„Čl. 7 (1) Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem."

„Čl. 10 (1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.

(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

(3) Každý má právo na ochranu před ***neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů*** *o své osobě."*[1]

Jak je uvedeno výše, dnem 1.6.2000 se v ČR účinná právní úprava ochrany osobních údajů zásadně rozšířila, jelikož tímto dnem vstoupil v účinnost *Zákon o ochraně osobních údajů, č.*

[1] Úplné znění Usnesení České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky

101/2000 Sb. (dále i jen ZOOÚ), který byl platný od 25.4. téhož roku. Zároveň s účinností ZOOÚ byl zřízen *Úřad pro ochranu osobních údajů* (ÚOOÚ) jako **nezávislý správní orgán** v oblasti ochrany osobních údajů, který dozoruje dodržování povinností stanovených zákonem v oblasti zpracování osobních údajů (ÚOOÚ, 2018b).

ZOOÚ byl od doby svého vzniku průběžně aktualizován (celkem proběhlo dvacet pět aktualizací) a v současné době se vytváří nový zákon, který ho nahradí a ZOOÚ tak pozbyde platnost.

V Evropské Unii mezitím došlo k dalšímu vývoji v této právní oblasti, a to vytvořením *Směrnice 95/46 ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů* (neboli *Evropská směrnice o ochraně osobních údajů*), platná od 13. prosince 1995 až do května roku 2018. Je nutné věnovat pozornost slovu „směrnice" v názvu, neboť to znamená, že členské státy byly povinny podle ní **uvést svoji legislativu do souladu**, není přímo právně účinná pro jednotlivé subjekty.

Tato směrnice hrála důležitou roli v utváření následující legislativy prostřednictvím článku 29:

„Článek 29

Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů

1. Zřizuje se pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů (dále jen „pracovní skupina"). Pracovní skupina má poradní funkci a je nezávislá.

2. Pracovní skupinu tvoří zástupce orgánu dozoru nebo orgánů dozoru určených jednotlivými členskými státy, zástupce orgánu nebo orgánů vytvořených pro orgány a instituce Společenství a zástupce Komise.".[2]

Pro pracovní skupiny zřízenou článkem 29 se vžilo označení *WP29* a od roku 1997 produkovala množství stanovisek k aktuálním problémům. Když začalo opětovné přehodnocování stávající evropské legislativy v oblasti ochrany osobních údajů, WP29 spolupracovala na vytváření **nového právního dokumentu**, který razantně zasáhne právo napříč celým světem.

---

[2] SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 95/46/ES ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů; (Úř. věst. L 281, 23.11.1995, s.31-50)

2 CHARAKTERISTIKA A VYBRANÉ POJMY GDPR

Prvním oficiálním dokladem ohledně revize Evropské směrnice o ochraně osobních údajů je návrh předložený Evropskou komisí 25. ledna 2012. Návrh „Nařízení Evropského parlamentu a rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů)" vyplynul z mnoha jednání a dvou veřejných konzultací, jak je uvedeno v důvodové zprávě. Již od počátku se pracovalo s formou **nařízení**, podle návrhu se jedná o nejvhodnější právní nástroj, protože se na základě **přímé použitelnosti** *„omezí právní nejednotnost a zvýší právní jistota tím, že se zavede harmonizovaný soubor základních pravidel, zlepší ochrana základních práv jednotlivců a přispěje k fungování vnitřního trhu".*[3] Nařízení stanovuje práva a povinnosti přímo adresátům, bez ohledu na míru adaptace vnitrostátní legislativy. Jednotlivým **státům je ponechána pouze částečná možnost úpravy** ve stanovených oblastech. V roce 2012 zároveň pracovní skupina WP29 začala uveřejňovat stanoviska jako podporu vytvoření nařízení.

Po prvotním návrhu následovalo několik kol úprav a schvalování nejprve samostatně v Evropském parlamentu, Radě EU a v Evropské Komisi, následně už společné jednání v rámci takzvaného „trialogu". K završení procesu došlo v roce 2016 uveřejněním „Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)" v Úředním věstníku Evropské unie.[4] Tímto **vstoupilo Obecné nařízení o ochraně osobních údajů (dále jen GDPR) v platnost**, se stanoveným datem **nabytí účinnosti 25. května 2018**.

Svým obsahem je GDPR mnohem propracovanější než směrnice 95/46/ES. Jednou z nejvýraznějších kvalitativních změn oproti ní jsou podle Žůrka **princip odpovědnosti správce** a **přístup založený na riziku** (Žůrek, 2018). První z nich, princip odpovědnosti správce je popsán v čl. 24 odst. 1: *„S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen*

[3] Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) 5853/12, 27.1.2012, s.5. Dostupné z: http://data.consilium.europa.eu/doc/document/ST-5853-2012-INIT/cs/pdf

[4] Úřední věstník Evropské unie. L 119, svazek 59, 4.5.2016, české vydání. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=CS

doložit, že zpracování je prováděno v souladu s tímto nařízením." – cílem není jednorázová zpráva o situaci, ale soustavný proces správce nastavování a kontrolování probíhajících zpracování. Přístup založený na riziku je popsán v čl. 25 a čl. 32, stručně stanovuje správcům, aby na základě svých zpracování zvolili vhodná opatření – Obecné nařízení je možné aplikovat různými způsoby podle konkrétního předmětu a průběhu zpracování.

2.1 Působnost

Obecné nařízení dopadá v podstatě na všechny občany Evropské Unie, protože téměř každý ve větší či menší míře poskytuje osobní údaje jiným osobám. Palčivějším dotazem ale je, kdo se jím bude muset řídit? Na to nařízení odpovídá negativním vymezením tak, že v souladu s ním bude muset postupovat každá právnická a fyzická osoba, která zpracovává osobní údaje (viz definice níže) pro **jinou než osobní či domácí činnost.** Tato výjimka se nachází v recitálu 18, kde je přesně uvedeno: *„nařízení se nevztahuje na zpracování osobních údajů fyzickou osobou v rámci činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti, a tedy bez jakékoliv souvislosti s profesní nebo obchodní činností".*[5]

V samotném textu nařízení jsou hned v první kapitole otázce působnosti věnovány dva články. V článku 2 je specifikována věcná: *„...nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny"*[6], která je v této práci objasněna dále v textu a v článku 3 se předkládá (mediálně známá) skutečnost, totiž že Obecné nařízení se **vztahuje na zpracování údajů v Unii tak i ve třetích zemích**, pokud se týká **subjektů** (tedy občanů) **usazených v některém ze států EU.**

2.2 Zásady

Mnoho informací o GDPR na svých stránkách uveřejňuje Úřad pro ochranu osobních údajů, mezi nimi je i „Základní příručka k GDPR", která formou otázek a odpovědí popisuje mimo

---

[5] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), recitál (18), s. 3 – 4. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

[6] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 2, odst. 1., s. 32. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

jiné i **zásady, na kterých je obecné nařízení postaveno**. Podle ÚOOÚ je lze shrnout na následující:

- *„zákonnost, korektnost, transparentnost – správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně a korektně,*
- *omezení účelu – osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely,*
- *minimalizace údajů – osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány,*
- *přesnost – osobní údaje musí být přesné,*
- *omezení uložení – osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány,*
- *integrita a důvěrnost – technické a organizační zabezpečení osobních údajů.* " (ÚOOÚ, 2018c).

2.3 Definice zpracování

Ve smyslu Obecného nařízení zpracování **není** jakékoli nakládání s osobními údaji, ač to tak podle jeho definice může vyznít: *„jakákoliv operace...jako je shromažďování, zaznamenání, uspořádání, strukturování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, nahlédnutí, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.* "[7].

Zpracování osobních údajů je chápáno jako **systematická** činnost, kterou správce nebo zpracovatel provádí **za určitým účelem**.

2.4 Právní důvody zpracování

Dále je nutné znát **definice právních důvodů zpracování**. Ty jsou totiž **nutnou podmínkou** legálního zpracování, to znamená, že i pokud by byly všechny ostatní povinnosti splněny, bez právního důvodu se jedná o **protizákonné zpracování**. Podle ÚOOÚ lze osobní údaje zpracovávat, pokud je přítomen aspoň jeden z následujících právních důvodů:

- *„subjekt údajů udělil souhlas pro jeden či více konkrétních účelů,*

[7] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 4, bod 2, s. 33. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

- *zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,*
- *zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,*
- *zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,*
- *zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,*
- *zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů.* " (ÚOOÚ, 2018c).

2.4.1 Souhlas

Je také důležité definovat správně udělený souhlas, k čemuž GDPR v čl. 4 odst. 11 stanovilo podmínky **souhlasu, jako projevu vůle**, který musí být:

- svobodný,
- konkrétní,
- informovaný a
- jednoznačný.

Souhlas musí být potvrzený **jednoznačným pozitivním postupem** – tedy není možné za uživatele ve formulářích „předzaškrtnout" políčka s udělením souhlasu (tzv. opt-out), ale naopak zobrazit políčko **prázdné s možností označení**.

Pokud správce používá ke zpracování souhlas, což je velmi běžné k zasílání např. marketingových sdělení, musí jednoznačnému splnění těchto požadavků věnovat pozornost, neboť **důkazní břemeno o správnosti souhlasu je na jeho straně**. Je tedy nutné vést záznamy o udělených souhlasech včetně okolností, za kterých k nim došlo (např. znění smluvních podmínek v čase udělení) a osoby, která souhlas udělila.

Podle Nezmara (2018) jsou klíčové body k přezkoumání správnosti požadovaného souhlasu následující:

- nepodmíněný souhlas,

- aktivní opt-in,
- podrobný,
- pojmenovaný,
- dokumentovaný,
- snadno odvolatelný,
- souhlas udělený bez nerovnováhy ve vztahu.

Z těchto pomocných bodů je nutné podrobněji popsat požadavek na snadnou odvolatelnost. Ten je totiž specifikovaný v článku 7 GDPR, kde je uvedeno, že tento krok může být proveden kdykoli, a to **stejným způsobem** (resp. stejně snadno) jako byl souhlas udělen.

Dosavadní souhlasy, tj. udělené před účinností Obecného nařízení, zůstávají v platnosti, ale jen **pokud byly uděleny v souladu** s jeho požadavky.

2.5 Pojmy

V této kapitole jsou popsány základní definice a obsah pojmů používaných v Obecném nařízení. Většina byla přebraná z terminologie používané v právním prostředí již dříve, např. v českém Zákoně o ochraně osobních údajů.

2.5.1 Osobní údaje

Základním pojmem úpravy Obecného nařízení je osobní údaj. Definice zůstává stejná jako předtím, tedy že *„osobním údajem jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě"* a je uvedena v čl. 4 bodě 1. Zpracováním osobních údajů je operace s pomocí i bez pomoci automatizovaných postupů. Takzvaným **subjektem údajů** je fyzická osoba, které se údaje týkají. Z toho vyplývá, že se GDPR **nevztahuje na údaje o právnických osobách** – ovšem na údaje např. zaměstnanců nebo členů statutárních údajů ano.

2.5.2 Citlivé údaje

Kategorii osobních údajů, která se v českém prostředí podle ZOOÚ nazývá „citlivé údaje", upravuje i Obecné nařízení. V článku 9 odst. 1 definuje tzv. **zvláštní kategorii osobních údajů**: *„osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné*

identifikace fyzické osoby"[8]. Těmto vymezeným údajům GDPR přiznává **zvláštní status** a na správcích a zpracovatelích, kteří je zpracovávají, požaduje vyšší standart zabezpečení. Zároveň se na ně nevztahují klasické právní důvody zpracování (uvedené v další podkapitole), lze s nimi pracovat jen na základě některého ze **zvláštních právních důvodů** uvedených v čl. 9 odst. 2.

2.5.3 Práva subjektů

Obecné nařízení subjektům údajů přisuzuje celou řadu práv, na základě kterých mohou klást správcům **požadavky**, které musí být bez zbytečného odkladu zodpovězeny nebo provedeny a to **bezplatně**. V první řadě má subjekt právo na to **být informován**, což je pasivní právo – aktivitu pro poskytnutí nebo zpřístupnění informací musí vyvinout správce. Mezi další práva podle ÚOOÚ patří:

- *„právo na přístup k osobním údajům,*
- *právo na opravu, resp. doplnění,*
- *právo na výmaz,*
- *právo na omezení zpracování,*
- *právo na přenositelnost údajů,*
- *právo vznést námitku,*
- *právo nebýt předmětem automatizovaného individuálního rozhodování s právními či obdobnými účinky, zahrnujíce i profilování."* (ÚOOÚ, 2018d).

2.5.4 Správce a zpracovatel

Pro účely obecného nařízení se **správcem** rozumí *„subjekt, nerozhoduje jaké právní formy, který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá".*[9] Každé zpracování musí mít svého správce. Tento pojem se shoduje s českou definicí používanou v ZOOÚ.

Správce nezřídka není sám, kdo získané osobní údaje zpracovává – pokud si na určité činnosti najímá jiný subjekt, pak se jedná o **zpracovatele**. Ten nemůže předané osobní údaje

---

[8] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 9, odst. 1., s. 38. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

[9] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 4, bod 7, s. 33. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

využít pro své potřeby, ale pouze pro účely stanovené správcem. Je nutné při výběru zpracovatele dbát na kvalitu jeho služeb a úroveň zabezpečení poskytnutých osobních údajů.

K použití zpracovatele **není nutné získávat od subjektu údajů zvláštní souhlas**, protože zpracovatel, jak je uvedeno výše, využívá osobní údaje pouze pro účely správce. Obecné nařízení v čl. 28 odst. 3 vyjmenovává náležitosti, které musí splňovat **smlouva o zpracování osobních údajů**, což je podstatný instrument upravující vztah správce a zpracovatele. Definice pojmu zpracovatel zůstává stejná jako v ZOOÚ.

2.5.5 Dozorový úřad

V textu Obecného nařízení se hojně objevuje termín dozorový úřad. Na českém území tuto funkci zastává již zmiňovaný **Úřad pro ochranu osobních údajů**. V článku 57 jsou uvedeny jeho úkoly, například dozorový úřad:

a) „monitoruje a vymáhá uplatňování tohoto nařízení;

b) zvyšuje povědomí veřejnosti o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováním a podporuje porozumění těmto otázkám. Zvláštní pozornost se přitom věnuje akcím, které jsou určeny speciálně pro děti;

c) v souladu s právem členského státu poskytuje poradenství vnitrostátnímu parlamentu, vládě a dalším orgánům a institucím ohledně legislativních a správních opatření týkajících se ochrany práv a svobod fyzických osob v souvislosti se zpracováním;

d) podporuje povědomí správců a zpracovatelů o jejich povinnostech podle tohoto nařízení.“[10]

Za uvedenými prvními čtyřmi úkoly následuje mnoho dalších, přičemž provádění těchto úkonů je pro subjekty údajů **bezplatné**.[11] Mezi další jeho nápravné pravomoci patří **udělování pokut**, což je velmi diskutovaná stránka zavádění Obecného nařízení. Stanovená maximální výše je totiž pro české právní předpisy přinejmenším nezvyklá, a to 20 000 000 EUR, resp. pokud se jedná o podnik, až do výše 4 % celkového ročního obratu celosvětově, podle toho, která hodnota je vyšší. Druhy porušení jsou rozděleny do dvou kategorií, přičemž v první

---

[10] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 57, odst. 1, s. 68. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

[11] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 57, odst. 3, s. 69. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

kategorii je maximální výše sankcí poloviční oproti výše uvedeným hodnotám, tj. 10 000 000 EUR, resp. 2 % ročního obratu.

Ačkoli obě tyto částky jsou pro správce oprávněně nepříjemnou představou, Obecné nařízení v článku 83, který se zabývá podmínkami udělování pokut, obsahuje ustanovení, která jednak zajišťují spravedlivé udělování: *„každý dozorový úřad zajistí, aby ukládání správních pokut (...) bylo v každém jednotlivém případě účinné, přiměřené a odrazující"*[12] a jednak umožňují, aby k uložení pokuty vůbec nemuselo dojít: *„pokuty se ukládají podle okolností každého jednotlivého případu kromě či namísto opatření uvedených v čl. 58 odst. 2 písm. a) až h) a j)"*[13].

V odkazovaných písmenech článku 58 odst. 2 je uvedena řada **nápravných opatření**, která dozorový úřad (ÚOOÚ) může vůči správcům a zpracovatelům při porušení Obecného nařízení udělit, a to např. udělit napomenutí, nařídit opravu či výmaz osobních údajů nebo pouze upozornit, že zamýšlené zpracování pravděpodobně porušuje nařízení.[14]

2.6 *Předávání údajů mimo tuzemsko*

Pokud se údaje ke zpracování předávají v rámci zemí Evropské unie, není zapotřebí (kromě právního důvodu) žádných dodatečných opatření díky volnému pohybu osobních údajů. Pokud je nutné předávat údaje mimo EU, musí být adekvátně zajištěna jejich bezpečnost.

Zvláštní výjimka se týká třetích zemí, které v Úředním věstníku Evropské unie uvádí Evropská komise jako ty, ve kterých je ochrana osobních údajů dostatečná a je možné postupovat jako při běžném předávání mezi správci, resp. správcem a zpracovatelem. Tyto země jsou zveřejněny i na webových stránkách Úřadu (ÚOOÚ, 2018e) (tzv. **rozhodnutí o odpovídající ochraně**). Tamtéž jsou zveřejněny i **podmínky předání** do ostatních zemí, které můžou být podle jedné z následujících možností:

- předání založené na vhodných zárukách,
- závazná podniková pravidla,

---

[12] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 83, odst. 1, s. 82. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

[13] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 83, odst. 2, s. 82. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

[14] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 58, odst. 2, s. 69. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

- standardní smluvní doložky
- výjimky pro specifické situace, kdy nelze aplikovat jeden ze dvou shora uvedených bodů.

3 VLIV GDPR NA E-COMMERCE

V další části práce je e-commerce rozebrána z různých pohledů a uveden vliv Obecného nařízení na jednotlivé oblasti a činnosti.

E-commerce (neboli elektronické obchodování) má řadu definic, v českém prostředí je jedna z používaných například tato: *„E-commerce rozumíme využívání informačních a komunikačních technologií v procesech prodeje a nákupu, tj. v obchodní transakci."* (Jandoš, 2001).

Definice OECD dělí elektronické obchodování podle míry zahrnutí internetu na širší a užší pojetí. Užší definice zní následovně: *„Internetová transakce je prodej či nákup výrobků a služeb, ať už mezi podnikateli, domácnostmi, jednotlivými spotřebiteli, vládou, dalšími veřejnými či soukromými organizacemi, který je prováděn prostřednictvím internetu. Výrobky a služby jsou objednávány prostřednictvím internetu, ale vlastní dodávka výrobku či služby může být provedeno on-line nebo off-line."* (Sedláček, 2001).

Posuzovat zvlášť vliv GDPR na e-commerce odděleně od ostatních způsobů obchodování je smysluplné, protože elektronický obchod má svá specifika v komunikaci (tedy přenosu dat, potažmo osobních údajů) probíhající nepřetržitě **24 hodin denně** a často v **reálném čase** a využívá mnohé komunikační prostředky. (Janouch, 2014)

3.1 Modely e-commerce

Jako jiné obchodování, i tento obor se dá rozdělit na různé modely, z nichž podle Sedláčka (s. 97, 2001) nejpoužívanější jsou **B2B (trh pro firmy) a B2C (prodej koncovému spotřebiteli).** V první části práce bylo již naznačeno, že nová právní úprava nedopadá stejně na oba modely, neboť znatelně více postihuje podniky, které prodávají své zboží nebo služby **fyzickým osobám** – spotřebitelům, ale i živnostníkům.

Při podnikání v modelu B2B je jednodušší zejména **oslovování potenciálních klientů** pomocí internetu, telefonu nebo jiných podobných metod – lze použít veškeré veřejně dostupné informace o právnických osobách. Osobním údajem jsou až **informace o fyzických osobách**, tj. zaměstnancích, jednatelích, majitelích apod. V českém prostředí je ale nutné brát na zřetel Zákon č. 480/2004 Sb., o některých službách informační společnosti.

Pro komunikaci s fyzickými osobami při B2C platí všechna omezení uvedená na předchozích stránkách. Podnik musí ke zpracování jakýchkoli údajů mít **legitimní důvod** a např. při používání souhlasu se nesmí stát, že údaje poskytnuté k určitému účelu budou

využívány i jinak. Ve zkratce, pokud (potenciální) zákazník nedá **specifický aktivní souhlas** se zasíláním obchodních informací a uchováváním kontaktu v databázi, správce ho musí zničit (pokud ke zpracování nemá jiný právní důvod).

3.2 Marketing

Samozřejmě Obecné nařízení dopadne nejvíce na činnosti podniku, které se bez osobních údajů subjektů neobejdou – zejména **marketing**. Internetový marketing je podle Janoucha (2014) způsob, jakým lze dosáhnout požadovaných marketingových cílů prostřednictvím internetu a zahrnuje celou škálu aktivit spojených s **ovlivňováním, přesvědčováním a udržováním vztahů se zákazníky**. On-line cílení obsahu, podpora prodeje pomocí výherních akcí za poskytnutí e-mailu, zasílání newsletterů, to vše je forma e-marketingu, který s nástupem GDPR doznal podstatných změn.

Jedna z výrazných změn je při sběru e-mailů od *potenciálních* zákazníku (tj. takových, kteří doposud nenavázali s podnikem žádný vztah a ten tak nemá oprávněný zájem je kontaktovat). Doposud patřilo k rozšířeným praktikám poskytovat **rozšířené služby za poskytnutí kontaktních údajů** – typickým příkladem je zaslání e-booku za poskytnutí e-mailu (mediaguru.cz, 2019). Tomu nastal účinností Obecného nařízení konec, neboť není možné takto vymáhat osobní údaje (mezi které e-mail patří).

Dále není možné používat k propagaci kontaktní údaje získané k jiným účelům. Tím se v podstatě znemožní *přeprodávání* databází kontaktních údajů. Nařízení používání takových databází sice přímo nezakazuje, ale musí být řádně **právně ošetřeno**. To znamená potvrzení, že pořizovatel tyto údaje získal v souladu s legislativou (na základě souhlasu uděleného v místě sběru) a uvedl, že údaje budou použity pro marketingové účely třetími stranami. Pokud jsou tyto podmínky splněné, je nutné informovat subjekty podle článku 14 GDPR v **přiměřené lhůtě** po získání osobních údajů, ale nejpozději do jednoho měsíce.[15]

Zasílání obchodních sdělení zákazníkům, kteří již uskutečnili obchod (nebo poptávku, objednávku...) je možné zdůvodnit i **oprávněným zájmem obchodníka**. Zdaleka to ale neznamená, že v této oblasti nenastaly žádné změny. Obchodní sdělení totiž musí **přímo**

[15] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 14, odst. 3, s. 42. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

souviset s prodávaným zbožím nebo službou, které bylo poskytnuto v rámci plnění, díky kterému byly získané kontaktní údaje zákazníka (epravo.cz, 2018a)

U online reklamy se vliv Obecného nařízení projeví v závislosti na tom, zda vyžaduje nebo nevyžaduje **profilování**. U reklamy, kde se obsah zobrazuje na základě jiného výběru (např. kontextová reklama, segmentovaná reklama) jejich personalizace neklade dodatečné podmínky. Naopak u behaviorálních reklam, kde se obsah vybírá pomocí zájmů uživatele odvozených z jeho chování je vyžadován souhlas subjektu specificky pro tuto činnost (Horák, 2017).

3.2.1 Zpracování pro účely přímého marketingu

Pro oblast e-komerce je charakteristické využívání přímého marketingu. Přímý marketing se popisuje jako *„způsob marketingové komunikace, při které se oslovují zákazníci přímým adresním oslovením"* (Žůrek, 2018). Oslovení může probíhat nejen osobně, ale např. i přes SMS nebo e-mail. Je nutné ale oprávněný zájem správce nějak obhájit, zasílání obchodního sdělení je možné uskutečnit buď se **souhlasem adresáta**, nebo využitím tzv. **zákaznické výjimky**. Samozřejmě je zachované právo subjektu kdykoli požádat o výmaz z databáze adresátů marketingových sdělení.

V recitálu 47 Obecného nařízení je uvedeno následující: *„zpracování osobních údajů pro účely přímého marketingu lze považovat za zpracování prováděné z důvodu oprávněného zájmu"*.[16] Jedná se o tzv. **zákaznickou výjimku**, podmínkami je, že zasílání obchodních sdělení má jasnou souvislost se službou nebo zbožím, který zákazník zakoupil a zároveň že zákazník mohl důvodně očekávat, že se stane poskytnutím kontaktních údajů adresátem marketingových sdělení (epravo.cz, 2018a). Toto platí za předpokladu, že zákazníkem je fyzická osoba. U právnických osob (neboli B2B marketingu) jsou pravidla GDPR volněji aplikovatelná, jelikož právnická osoba není subjektem údajů, její zaměstnanci ale již jsou. Zde je především nebezpečí nesouladu se zákonem č. 480/2004 Sb., o některých službách informační společnosti.

Souhlas k použití osobních údajů k účelům přímého marketingu se formou neliší od souhlasu uděleného k jinému zpracování, i zde platí, že musí být **aktivní** (opt-in) a **dostatečně informovaný** – zákazník musí přesně vědět, komu a k jakému účelu souhlas dává. Také je

---

[16] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), recitál (47), s. 9. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

potřeba dodat, že ač zatím soudní rozhodnutí neurčilo přesný časový údaj uchovávání souhlasu, rozhodně není použitelný navždy a není vhodné zasílat marketingová sdělení založená na jediném neobnoveném souhlasu po dobu desítek let (gdpr.cz, 2018a).

3.3 Vliv GDPR na vztahy s dodavateli

Obecné nařízení klade na správce a zpracovatele nároky i v oblasti výběru dodavatelů. Je nutné zajistit, aby si všichni dodavatelé byli vědomi a dodržovali **zákonné požadavky**. Podniky jsou více než dřívější legislativou tlačeny k tomu si své dodavatele prověřovat, jelikož při nedostatečné vyvinuté aktivitě za porušení nařízení zodpovídá i odběratel (cyberinsurance.cz, 2018).

Je nutné od sebe oddělit institut dodavatele, který se při plnění smlouvy (resp. provádění svých služeb) může do styku s osobními údaji dostat pouze nahodile a zpracovatele, který je správcem najímán na činnost související se zpracováním osobních údajů. V prvním případě není kromě výše uvedeného zajištění (např. prohlášení) souladu s GDPR nutné přistupovat k dalším opatřením, může ale být vhodné zakotvit do uzavírané smlouvy ustanovení o dodržení standardů bezpečnosti apod. Pokud dodavatel systematicky přistupuje a zpracovává osobní údaje správce, musí mezi nimi dojít k uzavření **smlouvy o zpracování osobních údajů** podle článku 28 Obecného nařízení, nebo k zahrnutí jejích podmínek do uzavírané smlouvy o poskytování služeb (ÚOOÚ, 2018f).

V budoucnosti lze očekávat rozšíření **certifikátů** neboli osvědčení (pojmy jsou v následujícím textu používány jako ekvivalenty podle vzoru terminologie používané ÚOOÚ) o kompatibilitě procesů dodavatele s GDPR a prokazování souladu podle kodexů chování, viz recitál 81: *„Jednou z možností, jak prokázat, že správce plní příslušné povinnosti, je dodržování schváleného kodexu chování nebo schváleného mechanismu pro vydávání osvědčení zpracovatelem."*[17]

3.4 Kodexy chování

Tento instrument by měl plnit funkci **vodítka** pro jednotlivé sektory – správce v určitém oboru provádějící činnost stejného typu. Vytváření a přihlášení se k dodržování je dobrovolné

[17] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), recitál (81), s. 16. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

(helpgdpr.cz, 2019). Po podepsání kodexu se ale správce nebo zpracovatel vystavuje povinnosti podrobovat se kontrole jeho dodržování.

První kodexy byly vydány již v roce 2016, např. se jedná o kodex poskytovatelů cloudových služeb ve sdružení CISPE (cispe.cloud, 2019) V českém prostředí začátkem roku 2018 kodex vydalo Ministerstvo práce a sociálních věcí a je určený pro poskytovatele sociálních služeb, úřady a dotčené útvary MPSV apod. (MPSV, 2018a).

3.5 Osvědčení

Podobně jako kodexy chování, i vydání osvědčení je **dobrovolné** a mělo by být dostupné vzhledem k zohlednění specifických potřeb všech podniků. Slouží jako doklad, že činnosti zpracování jsou prováděné v souladu s Nařízením. Vydává se na dobu nejvýše tří let s možností obnovení.[18] Vydávání osvědčení budou provádět subjekty pověřené dozorovým úřadem nebo akreditované určeným vnitrostátním orgánem. V České republice je tímto orgánem Český institut pro akreditaci, o.p.s. (ČIA), v současnosti však ještě není možné ani podávat žádost o akreditaci, neboť podle vyjádření ČIA nejsou jednoznačně definovány požadavky a kritéria. Nejsou tedy prozatím žádné subjekty schopné tato osvědčení vydávat (ČIA, 2019).

3.6 Evidence osobních údajů

V Obecném nařízení na žádném místě nejsou definované konkrétní požadavky na evidenci zpracovávaných osobních údajů. Význam slova evidence je *„vedení záznamů, přehled"* (slovnik-cizich-slov.net, 2018) – jednoznačně tedy patří do zpracování osobních údajů podle definice uvedené v kapitole 2.3. Stejně jako na všechny ostatní případy zpracování se na vedení evidence vztahují zásady správného zpracování osobních údajů, kromě toho ale Obecné nařízení ani ÚOOÚ neposkytují konkrétní návod, ani nekladou přesné požadavky. Důvodem je zřejmě stejně jako v ostatních případech poskytnutí volnosti správcům k spravování uložených údajů podle vlastní potřeby.

Zásady zpracování jsou následující: *„zákonnost, korektnost, transparentnost; omezení účelu; minimalizace údajů; přesnost; omezení uložení; integrita a důvěrnost"* (ÚOOÚ, 2018c). V této kapitole týkající se evidence bude dán důraz zejména na přesnost, omezení uložení, integritu a důvěrnost. Ostatní zásady jsou buď více procesní a systémové (*zákonnost,*

[18] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 42, s. 58. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

korektnost, transparentnost; omezení účelu), anebo k jejich naplnění z většiny dochází již před samotným uložením dat *(minimalizace údajů)*.

3.6.1 Přesnost

Správce by měl dbát na přesnost sbíraných údajů a v rámci možností jejich přesnost ověřovat. Za ověřování se podle ÚOOÚ považuje např. kontrola údajů podle občanského průkazu (ÚOOÚ, 2018g), což je u většiny provozovaných e-shopů neadekvátní požadavek vzhledem k charakteru transakcí. V praxi by správce měl přijmout především opatření k opravě či výmazu údajů nepřesných nebo při jejich změně (MPSV, 2018b).

Do zásady přesnosti také spadá aktualizace dat. Obecné nařízení nepožaduje nepřetržitou kontrolu všech zpracovávaných údajů, ponechává správci možnost zajistit kontrolu správnosti získaných údajů tak, aby došlo k naplnění zásady (ÚOOÚ, 2018h). Je tedy ponecháno na podnikateli, aby posoudil, zda a jak často bude ve svých databázích obchodních partnerů nebo zaměstnanců provádět aktualizace za účelem správnosti údajů.

3.6.2 Integrita a důvěrnost

Tato zásada ztělesňuje technické a organizační zabezpečení údajů, což je zásadní téma nejen pro mnohé provozovatele e-shopů. Technické prostředky, jak zabezpečit data ukládaná v elektronickém formátu, byly popsány v kapitole 4.2, u evidence údajů se jedná zejména o jejich šifrování a zálohování. Organizačním zabezpečením se rozumí především omezení přístupu zaměstnanců k uloženým datům. Je vhodné rozdělit práva uživatelů tak, aby mohli s osobními údaji pracovat pouze do té míry, jak vyžaduje výkon jejich pracovního zařazení – např. umožnění editačního práva pouze předem určenému uživateli, nebo jen malé skupině. V některých případech je také třeba pořizovat záznamy o tom, kdo a jak údaje upravoval, nebo s nimi jinak pracoval (ÚOOÚ, 2018g).

Při předávání údajů je vhodné mít smluvně zakotvenou přiměřenou ochranu údajů. Ačkoli za zpracování primárně odpovídá správce, podle článku 32 Obecného nařízení je za přijetí opatření k dostatečnému zabezpečení osobních údajů odpovědný zpracovatel.[19]

---

[19] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 32, s. 51. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

3.6.3 Omezení uložení

Podle této zásady by data měla být uložena pouze na dobu nezbytně nutnou. Příručka vytvořená Ministerstvem průmyslu a obchodu uvádí jako příklad jednorázový nákup v e-shopu, po jehož uskutečnění by údaje zákazníka měly být uchovávány pouze po dobu nezbytně nutnou pro uplatnění nároku z vad zboží, resp. po dobu, po kterou zákazník udělil souhlas se zasíláním obchodních sdělení. Uložení osobních údajů po delší dobu je možné z titulu oprávněného zájmu správce, který ale musí být přesně definovaný a srozumitelně zákazníkovi vysvětlený (MPSV, 2018b). Po uplynutí nezbytně nutné doby uložení by osobní údaje měly být smazány, nebo anonymizovány, aby nebylo možné podle nich identifikovat určitou osobu (ne pseudonymizovány).

3.6.4 Výmaz údajů

Již je zde zmíněno tzv. právo být zapomenut neboli povinnost správce provést výmaz osobních údajů, pokud o to subjekt požádá. Toto právo je ustanoveno článkem 17 Obecného nařízení.

Pro provozovatele e-shopů nejspíš vymazávání údajů na požádání bude výjimečnou situací. Ovšem vzhledem k tomu, že se jedná o naprosto novou možnost zavedenou GDPR, vyplatí se na ni předem připravit. Nařízení navíc stanovuje poměrně krátkou lhůtu na provedení výmazu – od obdržení žádosti má správce jeden měsíc na jeho uskutečnění a zároveň musí informovat žadatele, tedy subjekt údajů, o provedených opatřeních.[20]

Po obdržení žádosti je nutné přezkoumat její oprávněnost, právo na výmaz totiž není právem absolutním. Nejprve je vhodné si ověřit totožnost žadatele, zda se jedná o osobu způsobilou o výmaz žádat. Následně přichází na řadu zmapování veškerých zpracovávaných osobních údajů subjektu. V mnoha případech nebude nutné ani možné plošně smazat veškerá data, smazat se můžou (a musí) jen taková, u kterých je splněna alespoň jedna podmínka z článku 17 odstavce 1 Obecného nařízení (ÚOOÚ, 2018i).

Ke smazání nedojde typicky v těchto případech:

- pokud se údaje zpracovávají pro plnění smlouvy (např. doručovací adresa),

[20] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 12, s. 39. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

- u údajů nutných ke splnění zákonné povinnosti (archivace daňových a účetních dokladů, záznamová povinnost k sociálnímu a zdravotnímu pojištění u zaměstnanců),
- pokud převažuje oprávněný zájem správce nad zájmem subjektu údajů - například e-mailová komunikace ohledně náležitostí smlouvy nebo uskutečnění plnění (podnikatel.cz, 2018a).

Po reálném vymazání dat a bezpečné likvidaci všech dokumentů musí dojít k informování žadatele o podrobnostech procesu – konkrétně jaké údaje byly smazány a u kterých k výmazu dojít nemohlo s uvedením právních důvodů proč musí být zpracovávány.

Poslední povinností správce je rozšíření uvedené v recitálu 66 Obecného nařízení. Tam je uvedeno, že: *„aby bylo v internetovém prostředí posíleno právo být zapomenut, mělo by být rozšířeno právo na výmaz tím, že by správce, který zveřejnil osobní údaje, měl povinnost informovat správce, kteří osobní údaje zpracovávají, aby vymazali veškeré odkazy na dané osobní údaje či veškeré jejich kopie nebo replikace"*.[21] Finálním krokem zpracovávání žádosti o výmaz by tedy mělo být informování všech zpracovatelů a správců, kteří mohli mít přístup k osobním údajům subjektu, o obdržení žádosti a o vhodných opatřeních k úplnému a správnému splnění povinnosti (bulletin-advokacie.cz, 2017).

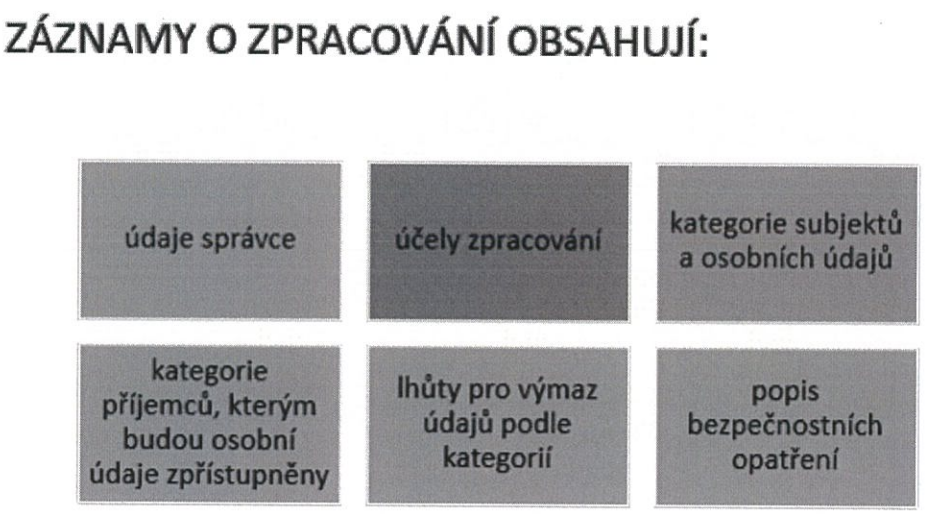
[21] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), recitál (66), s. 13. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

4 ZPRACOVÁNÍ E-SHOPU V SOULADU S GDPR

V této kapitole je uvedeno několik konkrétních případů, jak zpracovat vybrané funkcionality elektronického obchodu a nastavit vnitropodnikové činnosti tak, aby nedošlo k rozporu s Obecným nařízením. Uvedené informace jsou poté zpracovány i v grafické formě Návodu pro přípravu e-shopu v souladu s GDPR (dále i jen Návod), který je vcelku k práci přiložen jako příloha.

4.1 Mapování

Jak již bylo uvedeno, prokazování souladu zpracování s Obecným nařízením by měla být činnost **soustavná a vždy prokazatelná.** Z toho důvodu je nutné ze všeho nejdříve provést tzv. mapování zpracování – zjišťování, v jakém rozsahu a při jakých operacích vlastně správce osobní údaje zpracovává (Žůrek, 2018). Jedním z jeho výstupů by měly být záznamy zpracování, vyžadované GDPR jako po správci, tak po zpracovateli. Jejich podoba je v této práci konkrétně popsaná v kapitole 4.3.1, v Návodu jsou jejich náležitosti popsány pouze v bodech, viz obrázek 1.



Obrázek 1: Záznamy o zpracování

Zdroj: vlastní zpracování

4.2 Zabezpečení

Úroveň požadovaného zabezpečení je dána zmiňovaným „přístupem založeným na riziku". Povinnost zabezpečit je v článku 32 odst. 1 specifikována takto: *„s přihlédnutím ke stavu*

techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku".[22] Pro jednotlivé správce či zpracovatele je tedy zabezpečení osobních údajů posuzováno **individuálně**, dále jsou ale uvedeny možné příklady:

> *„a) pseudonymizace a šifrování osobních údajů;*
>
> *b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;*
>
> *c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;*[23]
>
> *d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.* "

Výše uvedené prvky nejsou povinné, ale správce odpovídá za přijetí adekvátních bezpečnostních opatření a musí být schopen doložit, že zpracování a jeho zabezpečení je v souladu s Obecným nařízením (ÚOOÚ, 2018j). To je uvedeno i v Návodu, společně s graficky zpracovanými příklady (viz obrázek 2) a informacemi ohledně incidentu.

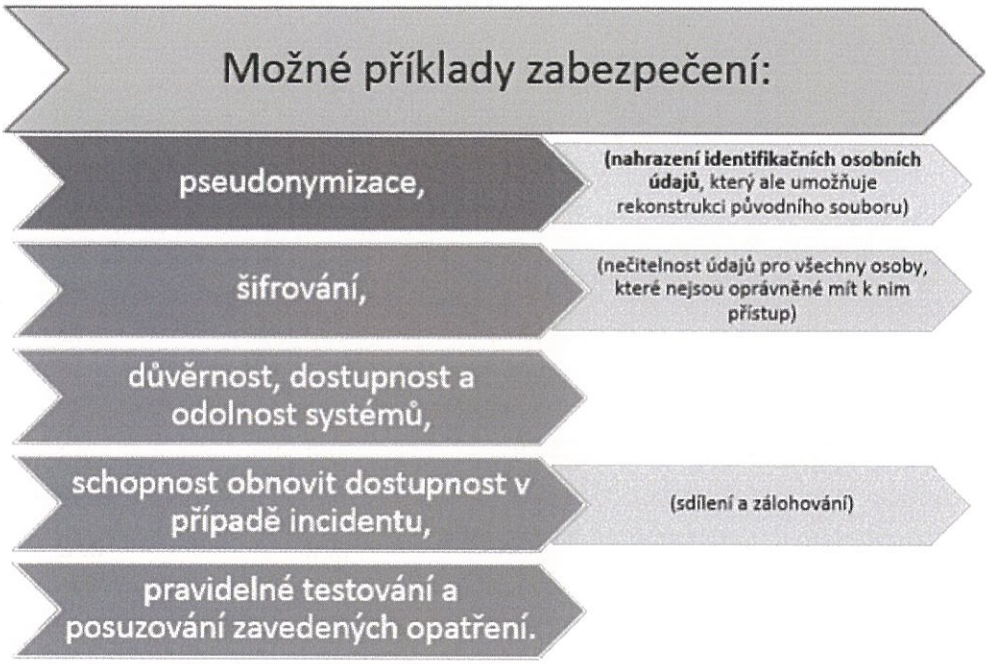
Na svých stránkách ÚOOÚ uvádí postup správců při porušení zabezpečení osobních údajů. Porušením je **incident**, který vede k zničení, ztrátě, změně nebo neoprávněnému poskytnutí zpracovávaných údajů. Pokud porušení představuje riziko pro práva a svobody fyzických osob, musí správce podat **ohlášení dozorovému úřadu** (ÚOOÚ), pokud se nejedná o bagatelní záležitosti. Pokud porušení představuje vysoké riziko, správci vzniká **povinnost zpravit subjekt údajů.**[24]

---

[22] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 32, odst. 1, s. 51. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

[23] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 32, odst. 1, s. 51–52. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

[24] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 34, odst. 1, s. 52. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.



Obrázek 2: Možné příklady zabezpečení

Zdroj: vlastní zpracování

4.2.1 Pseudonymizace

Proces **nahrazení identifikačních osobních údajů**, který ale umožňuje rekonstrukci původního souboru, se nazývá pseudonymizace. V Obecném nařízení je v článku 4 definován jako: *„zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě".*

Od anonymizovaných osobních údajů se liší tím, že se jedná o vratný proces. Kvůli tomu také pseudonymizované osobní údaje stále **podléhají GDPR** (gdpr.cz, 2018b). Technicky se provádí nahrazením identifikačních údajů jiným identifikátorem (pseudonymem), tento klíč se pak skladuje v odděleném souboru a je díky tomu možné s pseudonymizovanými údaji nakládat volněji (managementmania.cz, 2018).

4.2.2 Šifrování osobních údajů

Podle článku 34 odst. 3 jsou šifrované osobní údaje *„nečitelné pro všechny osoby, které nejsou oprávněny mít k nim přístup"*[25]. Rizikové kroky zpracování, které je vhodné zabezpečit pomocí šifrování jsou například **sdílení a zálohování**, nebo využívání **aplikačních a databázových serverů** (Nezmar, 2018). Obecně je doporučováno posílat elektronicky veškerá data zašifrovaná a heslo k přečtení předávat jiným kanálem.

Dále se doporučuje zabezpečit fyzická zařízení obsahující osobní údaje nebo umožňující přístup k nim ochránit proti vniknutí při zcizení. Pro šifrování mobilních telefonů a notebooků existují různé nástroje lišící se podle operačního systému zařízení.

4.3 Výčet potřebných dokumentů

Jak vyplývá z první části práce, soulad s Obecným nařízením je spíše věcí nastavení podnikových procesů než zahlcování právními dokumenty. Přesto je ale nejen pro dokázání souladu kontrolním orgánům vhodné připravit i v rámci malého e-shopu následující záznamy, které jsou popsané i v Návodu.

4.3.1 Záznamy o činnostech zpracování

Prvním takovým dokumentem, který slouží jak pro interní potřeby, tak ke zveřejnění veřejnosti jsou záznamy o činnostech zpracování.

Podle GDPR čl. 30 je povinností správce záznamy provádět. Tamtéž je uvedeno, jaké informace by měly obsahovat:

„a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;

b) účely zpracování;

c) popis kategorií subjektů údajů a kategorií osobních údajů;

d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;

---

[25] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 34, odst. 3, s. 53. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;

f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;

g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.“[26]

Účinností Obecného nařízení tyto záznamy **nahrazují oznamovací povinnost**, která byla správcům ustanovena ZOOÚ (ÚOOÚ, 2018k).

Z popisu obsahu záznamů výše vyplývá, že se nejedná o každodenní zaznamenávání dat, ale spíše o obecný výstup mapování sloužící pro orientaci ve zpracování osobních údajů a důkaz, že správce toto provádí řádně a v souladu s nařízením. Nebude se tedy sice pravděpodobně měnit často, ale je třeba ho **doplňovat a upravovat v návaznosti na aktuální průběh zpracovávání** osobních údajů správcem či zpracovatelem. Forma záznamů není stanovena, ale předpokládá se, že budou vyhotoveny písemně, resp. elektronicky.

Velký zájem je pochopitelně věnovaný odst. 5 čl. 30, který stanovuje **výjimky z povinnosti** vyhotovovat záznamy: *„Povinnosti uvedené v odstavcích 1 a 2 (tj. vedení záznamů) se nepoužijí pro podnik nebo organizaci zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů“.*[27] Výklad tohoto odstavce totiž není úplně jasný, žádné zpracování z definice nemůže být příležitostné, nešlo by tedy do této výjimky zařadit vůbec nic. Podle Žůrka (2018) je nutné výjimku vykládat v **souladu s účelem** – tedy by záznamy měly být vyhotoveny tam, kde je prováděno rozsáhlé zpracování a záznamy o činnostech zpracování tam budou plnit svou roli.

I přesto se doporučuje i podnikům, které by povinnost vést záznamy neměly, vyhotovit alespoň **stručný nástin činností zpracování**. Kromě dokazování souladu kontrolním orgánům

---

[26] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 30, odst. 1, s. 50-51. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

[27] Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů), čl. 30, odst. 5, s. 51. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

mají i další využití – firmy si utřídí povinnosti, vytvoří přehled a na základě získaných poznatků lze zefektivnit řízení (podnikatel.cz, 2018b).

4.3.2 Souhlas se zpracováváním

Dále je vhodné vypracovat vzorové souhlasy se zpracováním osobních údajů pro všechny činnost, u kterých je podle záznamů vyhotovených podle předchozí podkapitoly požadován.

Podmínky souhlasu musí být uvedené samostatně, nikoli jako součást všeobecných obchodních podmínek a musí být napsané pochopitelně, přehledně a co nejstručněji. V souhlasu musí být vždy uveden účel, a nikdy ne více najednou. Podle Obecného nařízení i vyjádření ÚOOÚ musí být souhlas *„udělen pro každý jeden konkrétní účel"*. (ÚOOÚ, 2018l).

Jak bylo uvedeno dříve v této práci, souhlasem nelze podmiňovat (ne)poskytnutí služby, měla by tedy být uvedena i možnost ho neudělit, také i postup, jak lze od udělení souhlasu odstoupit.

Kromě toho, že by tento dokument měl být vypracovaný podle zásad uvedených v kapitole 2.4.1, jsou doporučené náležitosti tyto:

- seznam zpracovávaných osobních údajů,
- účel zpracování (viz výše),
- doba platnosti souhlasu,
- identifikace správce a případných zpracovatelů,
- postup pro zrušení uděleného souhlasu,
- ev. předávání osobních údajů do třetích zemí. (blog.byznysweb.cz , 2018)

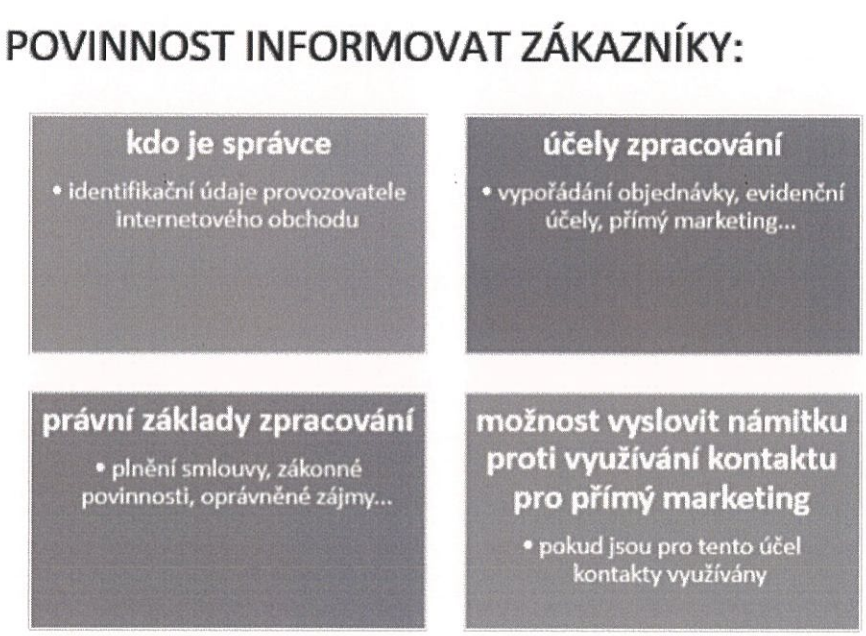
4.3.3 Veřejné dokumenty

Obecné nařízení na e-shopy klade nároky požadováním poskytování přehledných a úplných informací o zpracovávání osobních údajů. Záznamy o zpracování popsané v kapitole 4.3.1 slouží především k interním účelům, je ale nutné tyto informace předat i (potenciálním) zákazníkům a to ještě před odesláním objednávky (ÚOOÚ, 2018m). Jedním z řešení je vedle všeobecných obchodních podmínek (dále jen VOP), které jsou obvykle sestavované tak, aby naplnili povinnost prodejce podle § 1811 občanského zákoníku zveřejnit základní náležitosti smlouvy[28], vytvořit volně dostupné zásady zpracování osobních údajů. Jejich podoba se může

[28] Nový občanský zákoník 89/2012 Sb. Praha: Verlag Dashöfer, 2017.

lišit, v zásadě se ale bude jednat o (podle potřeby upravené) zásady o zpracování osobních údajů. Podle ÚOOÚ jsou minimem následující informace (grafické znázornění z Návodu je na obrázku 3):

- *„kdo je správce (identifikační údaje provozovatele internetového obchodu),*
- *účel zpracování (vypořádání objednávky, evidenční účely, přímý marketing),*
- *právní základ zpracování (plnění smlouvy se subjektem údajů, plnění právní povinnosti, oprávněné zájmy správce u přímého marketingu),*
- *možnost vyslovit námitku proti využívání kontaktu pro přímý marketing (pokud jsou kontakty využívány pro přímý marketing).* " (ÚOOÚ, 2018m)



Obrázek 3: Povinnost informovat zákazníky

Zdroj: vlastní zpracování

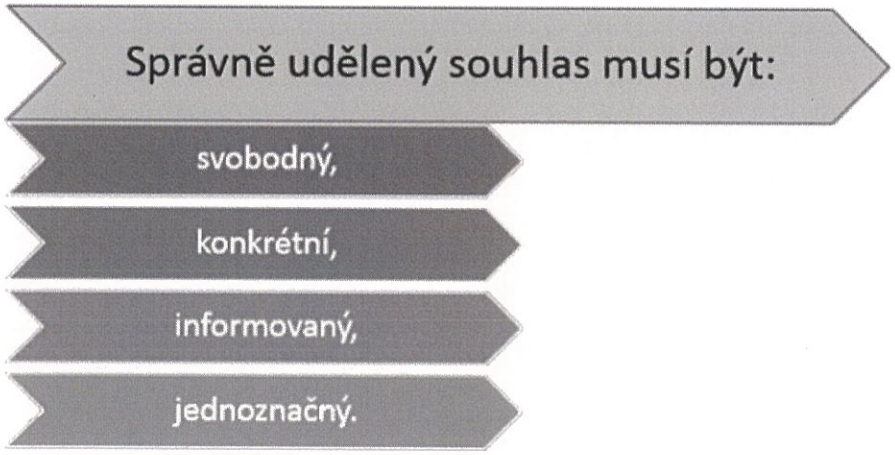
Další aktivitou nepřímo vyplývající z Obecného nařízení, ale doporučenou ÚOOÚ je informování návštěvníků stránek o druhu zpracovávaných cookies. Podrobný pohled na jejich využívání z pohledu GDPR je uvedený v kapitole 4.6.2 – zde jen stručně, pokud má uživatel v nastavení prohlížeče sběr cookies ke všem účelům povolen, pak se to považuje za poskytnutý souhlas a není nutné jej znovu vyžadovat při návštěvě konkrétní stránky.

Ve svém doporučení ke zpracování cookies ÚOOÚ uvádí, že by správce měl *„poskytnout informace o tom, v jakém rozsahu a pro jaký účel budou osobní údaje pomocí cookies*

zpracovány, kdo a jakým způsobem je bude zpracovávat a komu mohou být zpřístupněny, a to bez ohledu na právní základ zpracování těchto cookies, tedy včetně technických cookies" (ÚOOÚ, 2018n). Konkrétní podobou takové informace by mohla být tabulka rozčleněná podle jednotlivých druhů sbíraných cookies, ve které se s nimi zájemce seznámí a budou mu vysvětleny důvody, proč se tyto údaje sbírají a jak dlouho se uchovávají. Uvažovaným maximem a zároveň průmyslovým standardem doby archivování cookies je 13 měsíců (cnil.fr, 2019).

4.4 Získání souhlasu v souladu s nařízením

Pokud jsou podmínky souhlasu vypracované podle předchozí kapitoly (v Návodu jsou podmínky ve zkratce popsané jako na obrázku 4), je možné je uvádět při každé příležitosti, kdy je po zákazníkovi požadovaný. Například při nabídce zasílání newsletteru nebo jiných obchodních sdělení je možné uvést pouze platný odkaz na vypracovaný souhlas se zpracováváním osobních údajů **k tomuto účelu**.



Obrázek 4: Správně poskytnutý souhlas

Zdroj: vlastní zpracování

Správně vypracovaný vzor souhlasu se všemi náležitostmi sám o sobě nestačí, je nutné, aby byl také správně poskytnutý. Je proti nařízení, pokud je např. při vytvoření objednávky uveden podobný dodatek jako: „Odesláním objednávky uděluje zákazník souhlas se zpracováním svých osobních údajů za účelem zasílání newsletteru.", i kdyby následoval dotyčný odkaz (martindomes.cz, 2018a).

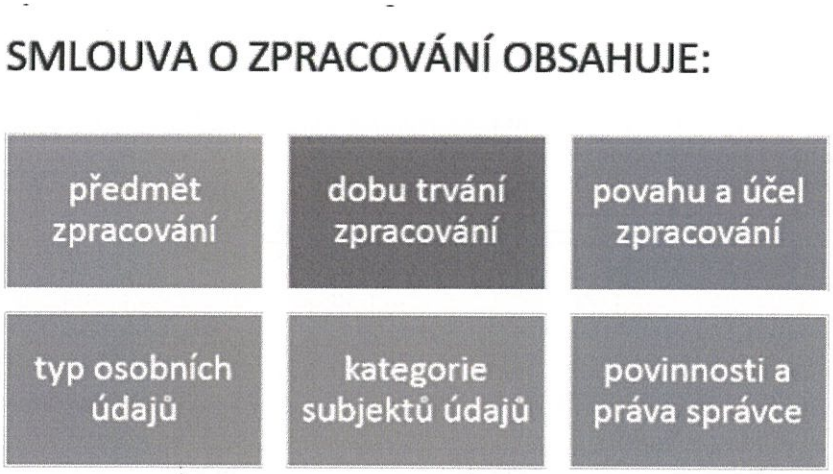
Další překážkou v získání souhlasu je notoricky známé zaškrtávací políčko. Objevuje se názor, že je nutné, aby bylo přítomné vždy, když se uděluje souhlas s osobními údaji. Pokud má ale formulář jen jeden účel (typicky zasílání newsletteru), pak se za aktivní souhlas považuje už samotné jeho vyplnění a odeslání, na správci ale stále zůstává informační povinnost (informovat zákazníka o náležitostech udělovaného souhlasu) a povinnost prokázat správnost uděleného souhlasu. Podle stanoviska pracovní skupiny WP29 to lze provést například takto: „*V on-line prostředí by správce například mohl uchovávat informace o relaci, ve které byl souhlas vyjádřen, společně s dokumentací o postupu získání souhlasu v době relace a kopii informací, jež byly tehdy subjektu údajů předloženy. Pouze odkázat na správnou konfiguraci příslušných internetových stránek by dostatečné nebylo.*" (ÚOOÚ, 2018o). Pokud je souhlas uveden v některém z kroků procesu uskutečnění objednávky, je zaškrtávací políčko samozřejmě nezbytné.

Speciální formou poskytování souhlasu je již jednou zmíněný princip double opt-in, tedy dvojnásobného aktivního potvrzení. Tento proces se používá při poskytování e-mailu a zamezuje uživateli vyplnit špatný kontakt. Po odeslání webového formuláře s vyplněnou e-mailovou adresou zákazník není uložen do databáze, ale je mu na uvedený e-mail zaslána ještě jedna potvrzující zpráva s odkazem, který musí otevřít v prohlížeči. Teprve po druhém kroku potvrzení je jeho e-mailová adresa zařazená do databáze např. k zasílání newsletterů (podle účelu uvedeného v souhlasu). Tím se eliminuje riziko, že uživatel úmyslně nebo omylem (např. překlepnutím) zadá špatný kontaktní údaj a tím postaví správce do role zasilatele neoprávněných sdělení, resp. zpracování osobních údajů bez relevantního právního důvodu zpracování (clipsan.cz, 2019).

Tento systém sice zvyšuje soulad s Obecným nařízením a je doporučovaný a podporovaný i ve vyjádřeních ÚOOÚ, v žádném případě ale není povinný (gdpr.cz, 2018c). Je čistě na správci, zda bude vyžadovat dodatečné potvrzení z e-mailu nebo pouhé odeslání webového formuláře.

4.5 *Smlouva o zpracování*

Další oddíl v Návodu ke zpracování e-shopu v souladu s GDPR je věnovaný vysvětlení pojmů správce a zpracovatel a možnému navázání smluvního vztahu mezi nimi. Na obrázku 5 jsou zobrazené náležitosti smlouvy o zpracování, které jsou také součástí Návodu.



Obrázek 5: Náležitosti smlouvy o zpracování

Zdroj: vlastní zpracování

4.6 *Vliv na jednotlivé kroky procesu nakupování*

Nakupování neboli realizování tzv. obchodního případu lze podle Sedláčka (2001) rozdělit například do **následujících čtyř fází**:

1. přípravná fáze (vyhledávání obchodních příležitostí),
2. kontrakční fáze (uzavírání smluvních vztahů),
3. realizační fáze (distribuce zboží),
4. finalizační fáze (převzetí zboží zákazníkem, popř. platba).

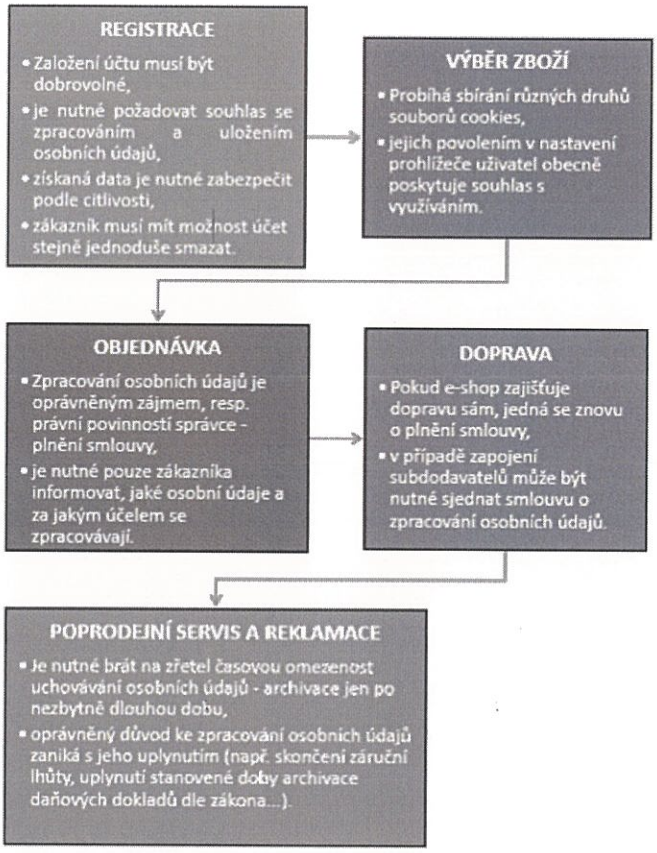
Jak probíhá nákup z pohledu zákazníka konkrétně v elektronických obchodech popisují např. Mikulášková a Sedlák (2015) v sedmi posloupných krocích tzv. objednávkového procesu:

1. nalezení nabídky e-shopu,
2. vyhledání zboží na e-shopu,
3. vložení zboží do košíku,
4. pokračování v nákupu nebo přechod k obsahu košíku,
5. potvrzení výběru zboží,
6. vyplnění fakturačních údajů,
7. odeslání objednávky.

Jelikož nákup zboží v e-shopu je poměrně unifikovaný proces, vyjmenované fáze jsou v dalším rozdělení nahrazeny pěti významnými „kroky", kterými zákazník prochází nebo které musí prodejce uskutečnit u většiny takto uskutečňovaných nákupů. Těmito etapami jsou:

1. registrace,
2. výběr zboží,
3. objednávka,
4. doprava a
5. poprodejní servis a reklamace.

V následujících podkapitolách je postupně popsán vliv GDPR na každou z nich. V Návodu jsou etapy rozdělené stejně a zpracovávání osobních údajů popsané zkráceně na základě těchto informací, jak je ukázáno na obrázku 6.



Obrázek 6: Zpracovávání osobních údajů podle fází nákupu

Zdroj: vlastní zpracování

4.6.1 Registrace

Při návštěvě e-shopu zákazníkem v modelovém případu má hned při vstupu na stránky možnost přihlášení do svého účtu nebo registrace, pokud účet ještě není vytvořený.

Pro zákaznické účty se typicky používají **osobní údaje** jako jméno, příjmení, adresa, ale některé e-shopy zahrnují také údaje o platební kartě. Při registraci je oproti dřívějšímu stavu v podstatě nutné požadovat **souhlas se zpracováním a uložením osobních údajů**. Založení účtu by mělo být dobrovolné a nesmí podmiňovat úspěšné dokončení nákupu (v B2C).

Co se týče zabezpečení ukládání dat z uživatelských účtů, je vhodné rozlišovat je podle **citlivosti a potenciálního nebezpečí** pro subjekt při úniku. Např. jména zákazníků můžou být přístupná všem zaměstnancům správce, platební informace, adresy a jiné osobní informace by měly být šifrované a ukládané odděleně (v případě potřeby pro interní analýzy apod. je možné využívat pseudonymizované údaje). Neexistují jednotné požadavky na technické zabezpečení zpracovávaných údajů, je tedy na posouzení správce nebo zpracovatele, jak s daty

z uživatelských účtů nakládat. Pro menší podniky a živnostníky může být jednodušší skladovat tato data v cloudovém úložišti, odpovědnosti se tímto způsobem sice zbavit nedá, ale poskytovatelé cloudových služeb mívají podobná opatření zavedená a ověřená audity a jinými certifikacemi (euro.cz, 2019).

Uživateli, který si založí účet by měla být dána i možnost **stejně jednoduše ho smazat** (tzv. právo být zapomenut) – toto se nevztahuje na údaje zpracovávané z jiného oprávněného důvodu (např. na základě uskutečněného nákupu).

4.6.2 Výběr zboží

Pro lepší poskytování služeb webové stránky včetně e-shopů od návštěvníků sbírají soubory **cookies**.

Jelikož cookies mohou obsahovat osobní údaje, vztahuje se i na ně Obecné nařízení. Rozlišují se ale podle účelu, ke kterému je provozovatel stránky sbírá, o každém je zákazníka nutné informovat zvlášť a na jejich zpracování se vztahují různé právní důvody.

Pro soubory cookies **nutné k provozu webu** nemůže být z logiky věci požadován souhlas, protože bez nich není možné poskytovat adekvátní služby. **K funkčním účelům**, jako je ukládání obsahu košíku v průběhu nákupu a standartnímu měření návštěvnosti lze použít právní titul oprávněný zájem (martindomes.cz, 2018b).

Kontroverzním druhem cookies jsou ty **sledovací používané k marketingovým účelům**. Už před vstupem Nařízení v účinnost byly občas k vidění „vyskakovací" lišty informující o sběru cookies k těmto činnostem, v první polovině roku 2018 se rozšířily na téměř všechny weby a často se k nim přidala okna umožňující uživateli poskytnout či odmítnout souhlas s využitím cookies k marketingu.

Současná právní úprava tyto automaticky se objevující lišty a okna neomezuje, není tedy možné říct, že by jejich použití bylo nesprávné. Podle stanoviska vydaného ÚOOÚ je ale zbytečné. Jelikož ukládání cookies si může každý uživatel řídit sám pomocí nastavení v prohlížeči, jejich povolení zde považuje za **obecně poskytnutý souhlas k jejich využívání** (ÚOOÚ, 2018n). Je otázkou, nakolik jsou s tímto postupem srozuměni návštěvníci webů jako subjekty údajů a zda jim takové uvažování přijde *správné*.

4.6.3 Objednávka

Pro zpracovávání údajů k provozování činnosti e-shopu jako je evidence zákazníků pro dodávání zboží, archivace daňových dokladů s osobními údaji pro plnění zákonné povinnosti atd. není již potřeba souhlas zákazníka, neboť je to oprávněným zájmem, resp. právní povinností správce. Je nutné zákazníka pouze informovat, jaké osobní údaje a za jakým účelem se zpracovávají (podnikatel.cz, 2018c).

Zde tedy oproti předešlému stavu došlo ke změně jednak v tom, že je nutné **revidovat nastavené procesy**, aby se zpracovávali jen osobní údaje skutečně nutné k odkazovanému procesu a jednak nelze podmiňovat uskutečnění objednávky vytvořením zákaznického účtu (gdpr.cz, 2018d).

Mnoho e-shopů využívá v případě prvního nákupu uživatele známou „léčku" – poskytnutí určité slevy výměnou za souhlas se zasíláním newsletterů a jiných nabídek na e-mail zákazníka. V tomto případě Obecné nařízení nic nemění, pro zákazníky se jedná o dobrovolný krok, který jim v případě odmítnutí konverzi neznemožní. Doporučuje se ale při využívání této strategie pro získání e-mailů do databáze používat tzv. „double opt-in", tedy zaslat potenciálnímu zákazníkovi po zadání kontaktu ještě zprávu s **potvrzujícím odkazem**, a až po druhém souhlasu e-mail zadat do databáze a zároveň poskytnout slevu (proficio.cz, 2018).

4.6.4 Doprava

Dalším krokem po vyřízení objednávky je nutnost **dopravení zboží zákazníkovi**. V případě, že e-shop si zajišťuje dopravu sám (typicky u zakázkové výroby dražších produktů apod.), neliší se zpracovávání údajů od předchozích kroků.

Tato činnost se začíná komplikovat v případě zapojení **subdodavatelů**, např. využívání poštovních služeb, kurýrů, soukromých dopravců aj. K tématu se vyjádřil ÚOOÚ na svém webu formou otázek a odpovědí takto: *„ V případě výkonu základních (poštovních) služeb spočívající pouze ve vlastním doručování zásilek, jde o samostatnou činnost dodavatele těchto služeb, tedy správce údajů, který provádí zpracování nebytné pro jím stanovený účel doručování.* " (ÚOOÚ, 2018p).

Pokud tedy dodavatel zajišťuje pouze samotnou fyzickou přepravu zboží z místa na místo, nejedná se o zpracovatele ve smysl GDPR. Obdrží sice jména a adresy adresátů, ty ale zpracovává jako **správce**, protože jsou nutné pro jeho soustavnou podnikatelskou činnost.

Aby se stal zpracovatelem, musel by s ním e-shop sjednat smlouvu **s dodatečným plněním**, kromě samotné přepravy i např. balení či tisk dokladů k zásilce. V takovém případě by bylo nutné uzavřít písemně smlouvu o zpracování osobních údajů podle čl. 28 Obecného nařízení, ve kterém jsou uvedeny požadované náležitosti takového dokumentu.

4.6.5 Poprodejní servis a reklamace

V oblasti uchovávání osobních údajů zákazníků po uskutečnění nákupu je největší změnou jeho **časová omezenost.** Archivace dat o nákupu a identifikačních údajů zákazníka může být uskutečňovaná z různých oprávněných důvodů, nejčastějším zřejmě bude *splnění právní povinnosti,* a to podle různých právních předpisů – např. archivace daňových dokladů podle Zákona o účetnictví a Zákona o dani z příjmu, podrobnosti o koupených výrobcích zase musí být dohledatelné v případě reklamace.

Pro všechny právní povinnosti platí, že jsou vymahatelné zpětně jen po určitý čas a oprávněný důvod ke zpracovávání údajů zaniká s jeho uplynutím (např. skončení záruční lhůty výrobku).

ZÁVĚR

Cílem práce je jednak ozřejmit pojem GDPR prostřednictvím vysvětlení pojmů a okolností vzniku, což je obsahem první a druhé kapitoly, jednak posoudit jeho vliv na e-commerce a vytvořit Návod pro zpracování e-shopu v souladu s pravidly Obecného nařízení, což je obsahem kapitol tři a čtyři.

GDPR, neboli Obecné nařízení o ochraně osobních údajů, je jako legislativa EU s přímou účinností na všechny občany Unie již od doby před vstoupením v platnosti předmětem široké diskuze. V začátku této práce byly popsány reálné důvody, proč bylo nutné takový právní předpis vytvořit z pohledu vývoje zpracovávání dat.

Po první kapitole, pojaté z historického hlediska, následuje charakteristika Nařízení z pohledu působnosti a jeho zásad. Součástí je vysvětlení nejdůležitějších pojmů, které se v textu Obecného nařízení vyskytují a identifikace osob, kterých se týká.

Následující kapitola byla věnována popisu vlivu GDPR na jednotlivé modely e-commerce a jeho dopadů na dva pravděpodobně nejvíce zasažené podnikové oblasti – marketing a evidenci osobních údajů (resp. jakoukoli evidenci, ve které se osobní údaje vyskytují).

Praktickou část práce tvoří Návod ke zpracování e-shopu v souladu s GDPR (dále jen Návod). V textu práce je nejdřív podrobně popsán, spolu s odkázáním na zdroje a rozdělen do kapitol a podkapitol v souladu s formou zbytku práce. Při zpracovávání Návodu byly využity teoretické poznatky z předchozích kapitol práce.

Graficky zpracovaný Návod je obsažen v příloze. Je jednoduchým orientačním návrhem především pro malé e-shopy, s vyznačením klíčových oblastí, které Nařízení postihlo a způsoby, jak upravit proces nákupu zákazníka tak, aby veškeré sbírané osobní údaje byly zpracovávané v souladu s GDPR, s řádným právním důvodem a adekvátním zabezpečením.

POUŽITÁ LITERATURA

KNIŽNÍ ZDROJE

JANOUCH, Viktor. Internetový marketing. 2. vyd. V Brně: Computer Press, 2014. ISBN 978-80-251-4311-7.

SEDLÁČEK, Jiří. E-komerce, internetový a mobil marketing. Praha: BEN - technická literatura, 2006. ISBN 80-7300-195-0.

MIKULÁŠKOVÁ, Petra a Mirek SEDLÁK. Jak vytvořit úspěšný a výdělečný internetový obchod. Brno: Computer Press, 2015. ISBN 978-80-251-4383-4.

ŽŮREK, Jiří. Praktický průvodce GDPR: včetně úplného znění GDPR. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9.

NEZMAR, Luděk. GDPR: Praktický průvodce implementací. Praha: Grada, 2017. ISBN 978-80-271-0668-4.

ELEKTRONICKÉ ZDROJE

(blog.byznysweb.cz, 2018) Jak připravit svůj e-shop nebo webovou stránku na GDPR?. Blog o podnikání na internetu [online]. Copyright © 2018 Podnikání na internetu [cit. 06.03.2019]. Dostupné z: https://blog.byznysweb.cz/2018/02/pripravte-svuj-e-shop-na-gdpr/

(bulletin-advokacie.cz, 2017) Právo být zapomenut :: Bulletin Advokacie. Bulletin advokacie, odborný právnický portál | Domů [online]. Dostupné z: http://www.bulletin-advokacie.cz/pravo-byt-zapomenut?browser=mobi

(cispe.cloud, 2019) CISPE CODE OF CONDUCT [online]. Dostupné z: https://cispe.cloud/code-of-conduct/

(clipsan.cz, 2019) Double opt-in? Jeho výhody a nevýhody (nejen) pro GDPR. [online]. Copyright © 2009 [cit. 06.03.2019]. Dostupné z: https://clipsan.com/blog/double-optin-gdpr/

(cnil.fr, 2019) Cookies: CNIL extends monitoring beyond website publishers | CNIL. CNIL | [online]. Dostupné z: https://www.cnil.fr/en/cookies-cnil-extends-monitoring-beyond-website-publishers

(cyberinsurance.cz, 2018) Jednoduchý průvodce GDPR. Co musíte už teď udělat, aby vaše firma vyhověla novým předpisům. | Cyberinsurance.cz. Cyberinsurance.cz | Blog o pojišťování kybernetických rizik [online]. Dostupné z: http://www.cyberinsurance.cz/?p=458

(ČIA, 2019) Český institut pro akreditaci, o.p.s. - Akreditace pro potřeby GDPR . Český institut pro akreditaci, o.p.s. - Český web [online]. Dostupné z: http://www.cia.cz/oznameni/akreditace-pro-potreby-gdpr.aspx

(epravo.cz, 2018a) GDPR a přímý marketing | epravo.cz. EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 03.12.2018]. Dostupné z: https://www.epravo.cz/top/clanky/gdpr-a-primy-marketing-107161.html

(euro.cz, 2019) 7 kroků, jak přežít GDPR: K lepší ochraně dat pomůžou cloud a šifrování (4) - Euro.cz. Euro.cz / Ekonomika, byznys, finance [online]. Dostupné z: https://www.euro.cz/byznys/7-kroku-jak-prezit-gdpr-k-lepsi-ochrane-dat-pomuzou-cloud-a-sifrovani-4-1374604

(gdpr.cz, 2018a) Stahují se mračna nad přímým marketingem? | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů — prakticky [online]. Copyright [cit. 03.12.2018]. Dostupné z: https://www.gdpr.cz/blog/direct-marketing/

(gdpr.cz, 2018b) Pseudonymizace osobních údajů | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů — prakticky [online]. Copyright © [cit. 03.12.2018].Dostupné z: https://www.gdpr.cz/gdpr/heslo/pseudonymizace-osobnich-udaju/

(gdpr.cz, 2018c) GDPR vnese pořádek do e-mailových databází | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů — prakticky [online]. Dostupné z: https://www.gdpr.cz/blog/gdpr-vnese-poradek-do-e-mailovych-databazi/

(gdpr.cz, 2018d) GDPR a e-shopy | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů — prakticky [online]. Dostupné z: https://www.gdpr.cz/blog/gdpr-e-shopy/

(helpgdpr.cz, 2019) GDPR krok za krokem - HelpGDPR.cz. GDPR krok za krokem - HelpGDPR.cz [online]. Copyright © Copyright 2000 [cit. 06.03.2019]. Dostupné z: https://www.helpgdpr.cz/gdpr/poradna.nsf/odpoved/jaky_je_rozdil_mezi_kodexy_chovani_a_osvedcenim_o_ochrane_osobnich_udaju__3418

(Horák, 2017) Co znamená GDPR pro online marketing - dopad na digitální ekonomiku. Jakub Horák - marketing a tvorba webových stránek [online]. Copyright © 2017 Webdesign by Jakub Horák. [cit. 06.03.2019]. Dostupné z: https://horakjakub.com/marketing/co-znamena-gdpr-pro-online-marketing/

(Jandoš, 2001) JANDOŠ, Jaroslav. Ke kořenům e-podnikání a e-obchodování. Business World. 2001(5), 25-29.

(managementmania.cz, 2018) Pseudonymizace (Pseudonymisation) - ManagementMania.com. [online]. Copyright © 2011 [cit. 03.12.2018]. Dostupné z: https://managementmania.com/cs/pseudonymizace-pseudonymisation

(martindomes.cz, 2018a) Jak na GDPR (3): Jak vypadá souhlas, o čem informovat a jak na PDF knížky. Martin Domes | webdesignér, lektor, autor knih [online]. Copyright © Martin Domes [cit. 06.03.2019]. Dostupné z: https://www.martindomes.cz/jak-na-gdpr-3-jak-vypada-souhlas-o-cem-informovat-a-jak-na-pdf-knizky/

(martindomes.cz, 2018b) Jak na GDPR (5): Cookies, Google Analytics, remarketing. Martin Domes | webdesignér, lektor, autor knih [online]. Copyright © Martin Domes [cit. 06.03.2019]. Dostupné z: https://www.martindomes.cz/jak-na-gdpr-5-cookies-google-analytics-remarketing/

(mediaguru.cz, 2019) S GDPR skončí některé marketingové triky | MediaGuru. Homepage | MediaGuru [online]. Copyright © 2019 [cit. 06.03.2019]. Dostupné z: https://www.mediaguru.cz/clanky/2018/03/s-gdpr-skonci-nektere-marketingove-triky/

(MPSV, 2018a) MPSV.CZ : Stanoviska a doporučené postupy. [online]. Dostupné z: https://www.mpsv.cz/cs/13916

(MPSV, 2018b) PŘÍRUČKA PRO PŘÍPRAVU MALÝCH A STŘEDNÍCH FIREM NA GDPR [online]. Ministerstvo průmyslu a obchodu. Copyright © [cit. 06.03.2019]. Dostupné z: https://i.iinfo.cz/files/podnikatel/631/prirucku-pro-pripravu-malych-a-strednich-firem-na-gdpr.pdf

(MVČR, 2001) Sdělení Ministerstva zahraničních věcí o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. Sbírka mezinárodních smluv č. 115/2001, částka 52, str. 2145. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=115/2001&typeLaw=mezinarodni_smlouva&what=Cislo_zakona_smlouvy

(podnikatel.cz, 2018a) Jak se v praxi poprat s žádostí o výmaz zákazníka podle GDPR? - Podnikatel.cz. Podnikatel.cz - největší server pro podnikatele v ČR [online]. Copyright © 2007 [cit. 06.03.2019]. Dostupné z: https://www.podnikatel.cz/clanky/jak-se-v-praxi-poprat-s-zadosti-o-vymaz-zakaznika-podle-gdpr/

(podnikatel.cz, 2018b) Jak se postavit k (ne)povinnosti vedení záznamů o činnostech zpracování? - Podnikatel.cz. Podnikatel.cz - průvodce vaším podnikáním [online]. Copyright © 2007 [cit. 04.12.2018]. Dostupné z: https://www.podnikatel.cz/clanky/jak-se-postavit-k-ne-povinnosti-vedeni-zaznamu-o-cinnostech-zpracovani/

(podnikatel.cz, 2018c) GDPR ochrana osobních údajů - GDPR a eshop,podejna - Podnikatel.cz. Podnikatel.cz - největší server pro podnikatele v ČR [online]. Copyright © 2007 [cit. 06.03.2019]. Dostupné z: https://www.podnikatel.cz/poradna/gdpr-ochrana-osobnich-udaju/180/

(proficio.cz, 2018) Jak sbírat e-mailové kontakty podle GDPR?. PROFICIO - Online marketing s entuziasmem [online]. Dostupné z: https://proficio.cz/jak-sbirat-e-mailove-kontakty-podle-gdpr

(slovnik-cizich-slov.net, 2018) evidence - význam slova | Slovník cizích slov. Slovník cizích slov .net - online hledání [online]. Dostupné z: http://www.slovnik-cizich-slov.net/evidence/

(ÚOOÚ, 2018a) Právní předpisy: Aplikace Úmluvy Rady Evropy č. 108 ve vztahu k povinnosti žádat Úřad o povolení k předání osobních údajů do zahraničí: Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 03.12.2018]. Dostupné z: https://www.uoou.cz/pravni-predpisy/ds-1257/archiv=0&p1=1657

(ÚOOÚ, 2018b) Historie Úřadu pro ochranu osobních údajů: Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 03.12.2018]. Dostupné z: https://www.uoou.cz/historie-uradu-pro-ochranu-osobnich-udaju/ds-1061/archiv=0

(ÚOOÚ, 2018c) 4. Zásady a právní důvody zpracování: Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 03.12.2018]. Dostupné z: https://www.uoou.cz/4-zasady-a-pravni-d-vody-zpracovani/d-27271

(ÚOOÚ, 2018d) Základní příručka k GDPR: Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 03.12.2018]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744

(ÚOOÚ, 2018e) Předávání založené na rozhodnutí o odpovídající úrovni ochrany osobních údajů: Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 03.12.2018]. Dostupné z: https://www.uoou.cz/predavani-zalozene-na-rozhodnuti-o-odpovidajici-urovni-ochrany-osobnich-udaju/ds-5065/p1=5065

(ÚOOÚ, 2018f) Zpracovatel: GDPR (obecné nařízení): Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 06.03.2019]. Dostupné z: https://www.uoou.cz/zpracovatel/d-29316/p1=3938

(ÚOOÚ, 2018g) GDPR stručně [online]. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 06.03.2019]. Dostupné z: https://www.uoou.cz/gdpr-strucne/ds-4843

(ÚOOÚ, 2018h) K problematice aktualizace zpracovávaných osobních údajů: GDPR (obecné nařízení): Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 06.03.2019]. Dostupné z: https://www.uoou.cz/k-problematice-aktualizace-zpracovavanych-osobnich-udaju/d-1595/p1=3938

(ÚOOÚ, 2018i) 6. Práva subjektu údajů: Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 06.03.2019]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276

(ÚOOÚ, 2018j) 8. Zabezpečení osobních údajů: Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 03.12.2018]. Dostupné z: https://www.uoou.cz/8-zabezpe-eni-osobnich-udaj/d-27282

(ÚOOÚ, 2018k) S účinností GDPR končí oznamovací povinnost správců: Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 04.12.2018]. Dostupné z: https://www.uoou.cz/s-ucinnosti-gdpr-konci-oznamovaci-povinnost-spravcu/d-28855

(ÚOOÚ, 2018l) K vyžadování souhlasu: GDPR (obecné nařízení): Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro

ochranu osobních údajů. Všechna práva vyhrazena. [cit. 06.03.2019]. Dostupné z: https://www.uoou.cz/k-vyzadovani-souhlasu/ds-5047/archiv=0&p1=3938

(ÚOOÚ, 2018m) Základní informace pro e-shopy . Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © [cit. 06.03.2019]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32710

(ÚOOÚ, 2018n) Doporučení k zpracování cookies a obdobných prostředků sledování od 25. května 2018. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © [cit. 06.03.2019]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29973

(ÚOOÚ, 2018o) PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright ©p [cit. 06.03.2019]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31896

(ÚOOÚ, 2018p) Zpracovatel: Heureka Shopping s.r.o. - zpracování osobních údajů v souvislosti se zasíláním dotazníků spokojenosti: Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 06.03.2019]. Dostupné z: https://www.uoou.cz/zpracovatel/d-29316/p1=5215

Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) 5853/12, 27.1.2012, s.5. Dostupné z: http://data.consilium.europa.eu/doc/document/ST-5853-2012-INIT/cs/pdf

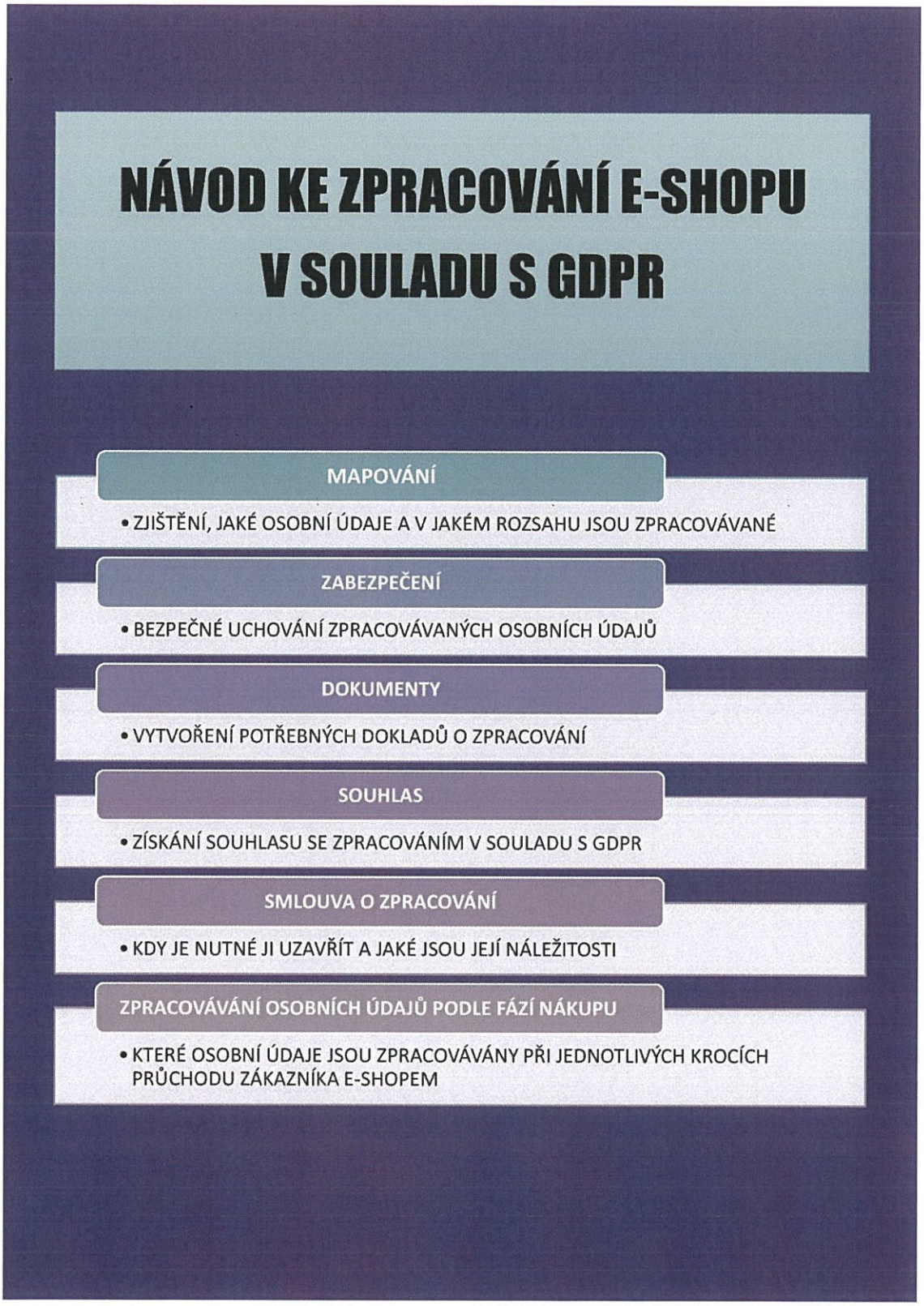
Nový občanský zákoník 89/2012 Sb. Praha: Verlag Dashöfer, 2017.

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 95/46/ES ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů; (Úř. věst. L 281, 23.11.1995, s.31-50)

Úplné znění Usnesení České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky

Úřední věstník Evropské unie. L 119, svazek 59, 4.5.2016, české vydání. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=CS

Příloha: Návod ke zpracování e-shopu v souladu s GDPR



MAPOVÁNÍ

V jakém rozsahu e-shop osobní údaje zpracovává?

Nalezení všech interních procesů, při kterých se zpracovávají osobní údaje.

Vytvoření záznamů o zpracování.

ZPRACOVÁNÍ

je systematické nakládání s osobními údaji za určitým účelem.

Např.: *shromažďování, zaznamenání, uspořádání, strukturování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, nahlédnutí, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.*

ZÁZNAMY O ZPRACOVÁNÍ OBSAHUJÍ:

údaje správce	účely zpracování	kategorie subjektů a osobních údajů
kategorie příjemců, kterým budou osobní údaje zpřístupněny	lhůty pro výmaz údajů podle kategorií	popis bezpečnostních opatření

ZABEZPEČENÍ

Správce odpovídá za přijetí ***adekvátních bezpečnostních opatření*** a musí být schopen doložit, že zabezpečení zpracování je v souladu s GDPR

=

zabezpečení je posuzováno ***individuálně***, nejsou stanovená ***žádná opatření povinná*** pro všechny.

Možné příklady zabezpečení:

- pseudonymizace, (**nahrazení identifikačních osobních údajů**, který ale umožňuje rekonstrukci původního souboru)
- šifrování, (nečitelnost údajů pro všechny osoby, které nejsou oprávněné mít k nim přístup)
- důvěrnost, dostupnost a odolnost systémů,
- schopnost obnovit dostupnost v případě incidentu, (sdílení a zálohování)
- pravidelné testování a posuzování zavedených opatření.

PORUŠENÍM ZABEZPEČENÍ je tzv. *incident* = událost, která vede ke zničení, ztrátě, změně nebo neoprávněnému poskytnutí osobních údajů.

Pokud porušení představuje riziko pro práva a svobody fyzických osob, musí správce podat ohlášení dozorovému úřadu (ÚOOÚ).

DOKUMENTY

I ty nejmenší elektronické obchody by měly připravit přinejmenším následující dokumenty:

1. **záznamy o činnostech zpracování** (obsah viz předchozí část mapování),
2. **vzorové souhlasy se zpracováním osobních údajů** (viz následující část souhlasy),
3. **veřejné informace** (viz níže).

POVINNOST INFORMOVAT ZÁKAZNÍKY:

kdo je správce

- identifikační údaje provozovatele internetového obchodu

účely zpracování

- vypořádání objednávky, evidenční účely, přímý marketing...

právní základy zpracování

- plnění smlouvy, zákonné povinnosti, oprávněné zájmy...

možnost vyslovit námitku proti využívání kontaktu pro přímý marketing

- pokud jsou pro tento účel kontakty využívány

SOUHLAS

Správně udělený souhlas musí být:

- svobodný,
- konkrétní,
- informovaný,
- jednoznačný.

SOUHLAS se zpracováním osobních údajů

je pouze jeden z možných právních důvodů zpracování. Dalšími jsou:

- plnění smlouvy uzavřené se subjektem údajů,
- splnění právní (zákonné) povinnosti,
- ochrana životně důležitých zájmů fyzické osoby,
- plnění veřejného zájmu nebo výkon veřejné moci,
- oprávněný zájem správce či třetí strany.

Doporučuje se vypracovat vzorové souhlasy se zpracováním osobních údajů pro činnosti u kterých je podle záznamů požadován.

Podmínky souhlasu musí být uvedené **samostatně**, (nikoli jako součást všeobecných obchodních podmínek), musí být napsané **pochopitelně**, **přehledně** a co **nejstručněji**. V souhlasu musí být vždy uveden **účel**, a nikdy ne více najednou.

Souhlasem nelze podmiňovat (ne)poskytnutí služby!

Při každé žádosti o souhlas by měla být uvedena i možnost ho neudělit, společně s postupem, jak lze od uděleného souhlasu odstoupit.

SMLOUVA O ZPRACOVÁNÍ

Subjekt, který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá je **správce** – ten zpracovává osobní údaje pro své účely.

Správce nezřídka není sám, kdo získané osobní údaje zpracovává – pokud si na určité činnosti najímá jiný subjekt, pak se jedná o **zpracovatele**. Ten nemůže předané osobní údaje využít pro své potřeby, ale pouze pro účely stanovené správcem.

SPRÁVCEM

je ohledně osobních údajů zákazníků, dodavatelů, zaměstnanců atd. typicky provozovatel e-shopu.

ZPRACOVATELEM

může být např. účetní, správce sítě, poskytovatel cloudu...

O využití zpracovatele **není nutné subjekt údajů informovat**, ale musí s ním být uzavřená smlouva o zpracování osobních údajů.

SMLOUVA O ZPRACOVÁNÍ OBSAHUJE:

- předmět zpracování
- dobu trvání zpracování
- povahu a účel zpracování
- typ osobních údajů
- kategorie subjektů údajů
- povinnosti a práva správce

ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ PODLE FÁZÍ NÁKUPU

REGISTRACE

- Založení účtu musí být dobrovolné,
- je nutné požadovat souhlas se zpracováním a uložením osobních údajů,
- získaná data je nutné zabezpečit podle citlivosti,
- zákazník musí mít možnost účet stejně jednoduše smazat.

VÝBĚR ZBOŽÍ

- Probíhá sbírání různých druhů souborů cookies,
- jejich povolením v nastavení prohlížeče uživatel obecně poskytuje souhlas s využíváním.

OBJEDNÁVKA

- Zpracování osobních údajů je oprávněným zájmem, resp. právní povinností správce - plnění smlouvy,
- je nutné pouze zákazníka informovat, jaké osobní údaje a za jakým účelem se zpracovávají.

DOPRAVA

- Pokud e-shop zajišťuje dopravu sám, jedná se znovu o plnění smlouvy,
- v případě zapojení subdodavatelů může být nutné sjednat smlouvu o zpracování osobních údajů.

POPRODEJNÍ SERVIS A REKLAMACE

- Je nutné brát na zřetel časovou omezenost uchovávání osobních údajů - archivace jen po nezbytně dlouhou dobu,
- oprávněný důvod ke zpracování osobních údajů zaniká s jeho uplynutím (např. skončení záruční lhůty, uplynutí stanovené doby archivace daňových dokladů dle zákona...).

COOKIES

mohou obsahovat os. údaje, GDPR se tedy vztahuje i na ně. Rozlišují se podle účelu, ke kterému je provozovatel webu sbírá a podle toho se na jejich zpracování vztahují různé právní důvody.

POUŽITÉ ZDROJE

7 kroků, jak přežít GDPR: K lepší ochraně dat pomůžou cloud a šifrování (4) - Euro.cz. Euro.cz / Ekonomika, byznys, finance [online]. Dostupné z: https://www.euro.cz/byznys/7-kroku-jak-prezit-gdpr-k-lepsi-ochrane-dat-pomuzou-cloud-a-sifrovani-4-1374604

8. Zabezpečení osobních údajů: Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 03.12.2018]. Dostupné z: https://www.uoou.cz/8-zabezpe-eni-osobnich-udaj/d-27282

Doporučení k zpracování cookies a obdobných prostředků sledování od 25. května 2018. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © [cit. 06.03.2019]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29973

GDPR ochrana osobních údajů - GDPR a eshop,podejna - Podnikatel.cz. Podnikatel.cz - největší server pro podnikatele v ČR [online]. Copyright © 2007 [cit. 06.03.2019]. Dostupné z: https://www.podnikatel.cz/poradna/gdpr-ochrana-osobnich-udaju/180/

GDPR vnese pořádek do e-mailových databází | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů — prakticky [online]. Dostupné z: https://www.gdpr.cz/blog/gdpr-vnese-poradek-do-e-mailovych-databazi/

Jak na GDPR (3): Jak vypadá souhlas, o čem informovat a jak na PDF knížky. Martin Domes | webdesignér, lektor, autor knih [online]. Copyright © Martin Domes [cit. 06.03.2019]. Dostupné z: https://www.martindomes.cz/jak-na-gdpr-3-jak-vypada-souhlas-o-cem-informovat-a-jak-na-pdf-knizky/

Jak na GDPR (5): Cookies, Google Analytics, remarketing. Martin Domes | webdesignér, lektor, autor knih [online]. Copyright © Martin Domes [cit. 06.03.2019]. Dostupné z: https://www.martindomes.cz/jak-na-gdpr-5-cookies-google-analytics-remarketing/

Jak připravit svůj e-shop nebo webovou stránku na GDPR?. Blog o podnikání na internetu [online]. Copyright © 2018 Podnikání na internetu [cit. 06.03.2019]. Dostupné z: https://blog.byznysweb.cz/2018/02/pripravte-svuj-e-shop-na-gdpr/

Jak se postavit k (ne)povinnosti vedení záznamů o činnostech zpracování? - Podnikatel.cz. Podnikatel.cz - průvodce vaším podnikáním [online]. Copyright © 2007 [cit. 04.12.2018]. Dostupné z: https://www.podnikatel.cz/clanky/jak-se-postavit-k-ne-povinnosti-vedeni-zaznamu-o-cinnostech-zpracovani/

K vyžadování souhlasu: GDPR (obecné nařízení): Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 06.03.2019]. Dostupné z: https://www.uoou.cz/k-vyzadovani-souhlasu/ds-5047/archiv=0&p1=3938

Nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů). Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=20112.

Pseudonymizace osobních údajů | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů — prakticky [online]. Copyright © [cit. 03.12.2018].Dostupné z: https://www.gdpr.cz/gdpr/heslo/pseudonymizace-osobnich-udaju/

Základní informace pro e-shopy . Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © [cit. 06.03.2019]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32710