Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Diplomová práce

Ochrana informací a dat u mobilního operátora

Bc. Michaela Barančinová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Michaela Barančinová

Veřejná správa a regionální rozvoj

Název práce

Ochrana informací a dat u mobilního operátora

Název anglicky

Information and data protection by mobile operator

Cíle práce

- seznámení s problematikou ochrany informací a dat u mobilního operátora
- zpřehlednění platné právní úpravy ochrany informací a dat v ČR
- identifikace problémů v oblasti ochrany informací a dat u mobilního operátora
- zjištění finanční náročnosti realizace ochrany informací a dat
- shrnutí výsledků s návrhy na opatření ke zlepšení zjištěných nedostatků

Metodika

- studium odborné literatury
- studium odborných článků a právních předpisů
- studium internetových odkazů
- popis
- vlastní šetření

- výklad práva (zejména logický, systematický, jazykový)
- komparativní metoda
- dotazníkové šetření

Doporučený rozsah práce

60-80

Klíčová slova

informace, data, mobilní operátor, poskytovatel, spotřebitel, ochrana spotřebitele, ochrana informací a dat, ochrana osobních údajů, finance

---

Doporučené zdroje informací

Bartík, V., Janečková, E., Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka 3. vydání, Praha: Linde Praha a. s. 2013, 311s. ISBN 978-80-86131-96-2

Dvořák, Jan – Švestka Jiří a kol.: Občanské právo hmotné 1, díl první: Obecná část, Wolters Kluwer a. s. ČR, 2013, s 430 ISBN 978-80-7478-326-5

Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, 536 s. ISBN 978-80-7179-226-0

Maisner, M., Vlachová, B.: Zákon o kybernetické bezpečnosti. Komentář. Praha: Wolters Kluwer, a. s. 2015. 232 s. ISBN 978-80-7478-817-8

Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, 468s. ISBN 978-80-7357-322-5

Novák, D.: Zákon o ochraně osobních údajů a předpisy související. Komentář. Praha: Wolters Kluwer, a. s. 2014, 504 s. ISBN 978-80-7478-665-5

Švestka, Jiří – Spáčil, Jiří a kol.: Občanský zákoník 1. § 1 až 459. Komentář. 2. vydání. Praha: C. H. Beck, 2009, 1394 s. ISBN 978-80-7400-108-6

Švestka, Jiří – Spáčil, Jiří a kol.: Občanský zákoník 2. § 460 až 880. Komentář. 2. vydání. Praha: C. H. Beck, 2009, 1114 s. ISBN 978-80-7400-108-6

Vaníček, Z., Mates, P., Nielsen, T.: Zákon o elektronických komunikacích. Komentář. Praha: Linde Praha a. s., 2014, 560 s. ISBN 978-80-7201-944-1

Zákon č. 101/2000 Sb., o ochraně osobních údajů ve znění pozdějších přepisů

Předběžný termín obhajoby

2017/18 ZS – PEF (únor 2018)

Vedoucí práce

Ing. JUDr. Pavel Pikola, Ph.D.

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 1. 11. 2017

JUDr. Jana Borská, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 1. 11. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 29. 11. 2017

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Ochrana informací a dat u mobilního operátora" jsem vypracoval(a) samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor(ka) uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30.11.2017 _____

Poděkování

Tímto bych ráda poděkovala JUDr. Ing. Pavlu Pikolovi PhD. za odbornou pomoc při zpracování mé diplomové práce. Dále tímto děkuji mým blízkým, kteří se mnou po celou dobu studií měli trpělivost.

V Praze dne 30.11.2017 _____

Ochrana informací a dat u mobilního operátora

Abstrakt

Diplomová práce se zaměřuje na platnou právní úpravu ochrany informací a dat zvláště v návaznosti na mobilního operátora. Analyzuje platnou právní úpravu v zákoně 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016, a zákonem č. 127/2005 Sb. o elektronických komunikacím, včetně zákona č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb. Jakožto členský stát EU je důležitou součástí platné právní úpravy i Směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů, která je platná do 25. května 2018, kdy vstoupí v platnost 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.

V praktické části se diplomová práce zaměřuje na mobilního operátora T-Mobile Czech Republic a.s. i v praxi, včetně dostupných procesů zaměřených na ochranu informací a dat. Součástí této části je osobní a dotazníkové šetření se zaměřením na ochranu osobních údajů. Tato část obsahuje zhodnocení získaných poznatků a výsledků.

Klíčová slova:

- poskytovatel
- spotřebitel
- ochrana spotřebitele
- ochrana informací a dat
- ochrana osobních údajů

Information and data protection by mobile operator

Abstract

The diploma thesis focuses on the valid legal regulation of the protection of information and data especially in relation to the mobile operator. It analyzes the valid legal regulation in Act 101/2000 Coll., On the Protection of Personal Data and on Amendments to Certain Acts, as amended from October 6, 2016, and Act No. 127/2005 Coll. on Electronic Communications, including Act No. 181/2014 Coll., on Cyber Security and on Amendments to Related Acts (the Cyber Security Act) as amended by Act No. 104/2017 Coll., Act No. 183/2017 Coll. and Act No. 205/2017 Coll. As an EU Member State, Directive 95/46 / EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which is valid until 25 May 2018 when it enters into force, is an important part of the current legislation Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In the practical part, the diploma thesis focuses on the mobile operator T-Mobile Czech Republic a.s. and in practice, including the available information and data protection processes. Part of this section is a personal and questionnaire survey focusing on the protection of personal data. This section contains an evaluation of the acquired knowledge and results.

Keywords:

- provider
- consumer
- consumer protection
- protection of information and data
- protection of personal data

Obsah

1 Úvod 11

2 Cíl práce a metodika 13
2.1 Cíl práce 13
2.2 Metodika 13

3 Teoretická východiska 15
3.1 Vývoj právní úpravy ochrany dat a informací 15
3.1.1 Platná právní úprava ochrany dat a informací v EU 15
3.1.2 Platná právní úprava ochrany dat a informací v ČR 16
3.2 Vymezení údajů 19
3.2.1 Osobní údaje 19
3.2.2 Identifikační údaje 20
3.2.3 Citlivé údaje 24
3.2.4 Práva a povinnosti správce osobních údajů 25
3.2.5. Povinnost správce likvidace osobních údajů 29
3.2.6. Dozorčí orgán pro ochranu osobních údajů 29
3.3 Ochrana dat a informací se zaměřením na mobilního operátora 31
3.3.1 Vývoj platné právní úpravy o elektronických komunikacích 31
3.3.2. Platná právní úprava zákona o kybernetické bezpečnosti 33
3.3.3. GDPR – Obecné nařízení o ochraně osobních údajů 40
3.4 Shrnutí 45

4 Vlastní práce 47
4.1 Mobilní operátor T-Mobile Czech Republic a.s. 47
4.1.1 Krátké představení mobilního operátora 47
4.1.2 Závěr představení mobilního operátora 51
4.2 Ekonomická část – Mobilní operátor součástí koncernu 51
4.3 Organizační struktura společnosti se zaměřením na bezpečnost 53
4.4 Ochrana osobních informací a dat procesně 55
4.4.1 Ochrana osobních údajů v praxi u T-Mobile 55
4.4.2 Proces anonymizace osobních údajů zákazníků 56
4.4.3 Bezpečnost informací a ochrana dat u mobilního operátora 58
4.5 Dotazníkové šetření 59
4.6 Anketa 65
4.7 Řízený rozhovor 67
4.8 Podíl mobilních a virtuálních operátorů na trhu v ČR porovnání s dotazníkovým šetřením 69

5 Poznatky a zhodnocení 75

6 Závěr 79

7 Seznam použitých zdrojů 81

8 Přílohy 84

Seznam grafů

Graf č. 1: Počet SIM karet …….. 70

Graf č. 2: Virtuální operátoři v síti T – mobile…… 71

Graf č. 3: Virtuální operátoři v síti O2 …… 72

Graf č. 4: Virtuální operátoři v síti Vodafone ……. 72

Graf č. 5: Struktura uživatelů mobilních telefonů v ČR (% z celkového počtu jednotlivců v dané socio-demografické skupin)…….....…… 73

Graf č. 6: Vybavenost domácností telefonem (% z celkového počtu domácností) …… .74

Graf č. 7: Vybavenost českých domácností telefony (% z celkového počtu domácností) 74

Seznam tabulek

Tabulka č. 1: Počet aktivních SIM karet ...…….69

Tabulka č. 2: Virtuální operátoři v síti T – mobile……..71

Tabulka č. 3: Virtuální operátoři v síti O2 ……..…….. 71

Tabulka č. 4: Virtuální operátoři v síti Vodafone ……. 72

1 Úvod

Téma ochrany osobních údajů je řadu let aktuální téma, a to nejen v České republice, ale i v celé Evropské unii. Tento problém byl řešen zvláště v souvislosti s mobilními operátory. Již několikrát v posledních letech vzniklo podezření na únik dat u mobilních operátorů a poslední podezření se i potvrdilo u společnosti T-Mobile Czech Republic a.s.

Rok 2016 byl ve znamení změn. Byla odsouhlaseno nové 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. Nařízení tzv. GDPR vstoupí v platnost ve všech členských státech k 25. květnu 2018, do té doby je nezbytná příprava, neboť se jedná o doposud největší převrat v ochraně osobních údajů a zároveň s tím vznikají státům i společnostem nové finanční zatížení. Cílem GDPR je hájit a chránit práva, větší přehlednost a kontrolu osobních dat všech občanů EU bez rozdílu. Tato revoluce v ochraně dat se bude dotýkat všech institucí, firem, online služeb i jednotlivců, kteří zpracovávají data uživatelů. Za porušování těchto nových a daleko přísnějších pravidel zavádí GDPR pokuty nezvykle vysokého charakteru a až čas ukáže, zdali toto nové nařízení splňuje předpokládanou maximální funkci ochrany. Nicméně do doby, než vstoupí v platnost toto nařízení se i nadále v České republice řídíme podle Směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016, a zákona č. 127/2005 Sb. o elektronických komunikacích.

V tomto roce postihl společnost T-Mobile Czech Republic a.s. únik dat, kdy jeden ze zaměstnanců se pokusil odcizit osobní údaje zákazníků a následně tyto data prodat. Jednalo se o zaměstnance, jenž se zákaznickými daty běžně pracoval. Společnost při podezření podnikla veškeré kroky pro zajištění těchto dat ve spolupráci s Policií České republiky. Mobilní operátor oznámil tuto skutečnost dle platné právní úpravu Úřadu na ochranu osobních údajů. Úřad k této skutečnosti vedl správní řízení a následně uložil pokutu ve výši 3,6 mil Kč. „Předmětem tohoto řízení byla skutečnost, že při zpracování osobních údajů svých zákazníků společnost T-Mobile Czech Republic a.s. nezajistila, aby nedošlo k úniku osobních údajů těchto fyzických osob, a to v rozsahu jméno, příjmení, datum narození, adresa, telefonní číslo, kód zákazníka, tarif, název, kategorie a značka zařízení,

údaj o průměrné útratě, platební metodě, popř. čísle účtu a kód banky.“[1] Z pohledu Úřadu na ochranu osobní informací došlo k nedostatečnému zabezpečení elektronické interní databáze. Je tomu skutečně tak, opravdu mobilní operátor dostatečně nezabezpečil přístup k osobním údajům svých zákazníků? Není spíše na vině nedostatečnost zákona, jež umožňuje takovéto praktiky v praxi? Cílem této práce je analyzovat situaci se zaměřením i na tyto zmiňované otázky.

[1] Úřad pro ochranu osobních údajů: Výroční zpráva 2016, dostupná z: https://www.uoou.cz/VismoOnline

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této práce je seznámení s platnou právní úpravou, a především pak jejím výkladem v oblasti ochrany osobních údajů a informací fyzických osob v České republice. Zvláště pak zmapování ochrany informací a dat při zpracování a nakládání s nimi u mobilního operátora. Práce je zaměřena na možné problémy v praxi zvláště pak v praktické části, kde budou analyzovány postupy nakládání s daty u mobilního operátora včetně procesů, které mají potvrdit nebo vyvrátit skutečnost, že mobilní operátor dostatečně nezabezpečuje data svých zákazníků. V případě prokázání nedostatečnosti zabezpečení bude navrhnuto, jak tuto situaci změnit.

2.2 Metodika

Metodika zpracování u této diplomové práce spočívala především u teoretické části ve shromažďování studijních materiálů, jejich následnému pečlivému prostudování a dalšímu zpracování poznatků tímto způsobem získaných. Zvláště byl použit systematický výklad práva pro rozbor legislativy, zejména se zaměřením na logický a jazykový výklad pro analyzování zákona 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších přepisů. Dále byl touto metodou zpracován i zákon 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a zvláště velký důraz byl kladen na Směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. U systematického rozboru Směrnic Evropského parlamentu a Rady byla požita zvláště i metoda historická, jež nám ukázala vývoj této legislativy. Po využití těchto metod pro výklad a analýzu byla zvolena pro další rozbor komparativní metoda, kterou bylo porovnáno, zdali se právní úprava pro Českou republiku liší od Směrnic Evropského parlamentu a Rady, jimiž je regulována ochrana osobních údajů a informací v rámci všech

členských států Evropské unie. Se zaměřením na systematický výklad bylo zpracováno i 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, jež vejde v platnost v květnu 2018.

V praktické části této diplomové práce je použita zvláště metoda analytická, jež vyplývá z vlastních zkušeností a stejně tak i vlastním šetřením u mobilního operátora společností T-Mobile Czech Republic a.s. Součástí této části zpřehlednění, jak nakládá operátor s daty a informacemi subjektů v praxi je i řízený rozhovor. Dále byla pro vlastní výzkum použita i metoda statistická včetně dotazníkového šetření, které mělo ukázat, jak jsou respondenti schopni vnímat důležitost ochrany svých dat a jejich základní přehled. Statistická metoda byla zároveň použita na zmapování trhu, kdy se stále navyšuje využití mobilních operátorů, což má vliv na gigantické množství dat a informací, jež má chránit mobilní operátor.

3 Teoretická východiska

3.1 Vývoj právní úpravy ochrany dat a informací

3.1.1 Platná právní úprava ochrany dat a informací v EU

Problematika ochrany osobních údajů se v minulosti řešila převážně na úrovni různých doporučení a stanovisek ze stran Komise Evropské unie a následně jí upravovala i „Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů vyžaduje, aby členské státy chránily práva a svobody fyzických osob v souvislosti se zpracováním osobních údajů, zejména jejich právo na soukromí, aby byl zajištěn volný pohyb osobních údajů ve Společenství.“[2] Z důvodu zrychlující se globalizace a zvláště vzhledem k pokroku technologického vývoje byla Evropská unie nucena se touto problematikou zabývat komplexněji a identifikovala nejzásadnější oblasti, jichž by se měla změna zmíněné směrnice z roku 1995 týkat. Evropská unie a k ní náležící orgány si kladly za cíl zvýšení transparentnosti pro subjekty údajů, dále byl kladen důraz na jednoznačné znění souhlasů se zpracováním osobních údajů subjektů. Samozřejmostí byla i snaha posílení práv subjekt, tzn. povinnost správce informovat subjekt o narušení bezpečnosti osobních údajů například při úniku dat, neoprávněném zničení. Dále minimalizovat množství údajů vzhledem k účelu, k němuž jsou správcem shromažďovány. Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, sjednocuje zvláště předpisy pro zajištění požadované přiměřené ochrany základních práv a svobod a to primárně práva na soukromí zvláště s ohledem na zpracování osobních údajů v odvětví elektronické komunikace.[3] Zvláště toto odvětví ochrany elektronických komunikací je změněno popřípadě doplněno ve Směrnici Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních kanálů, kdy tato změna vznikla z důvodu snahy o

[2] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, odst. 1

[3] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací čl. 1

sjednocení předpisů pro členské státy a úpravě povinností poskytovatelů veřejných komunikačních sítí a služeb elektronických komunikací, a to o ohledně uchovávání dat, ať už jimi vytvořených či uchovávaných. Cílem byla i dostupnost těchto údajů pro možnosti vyšetřování, odhalování i stíhání závažných trestných činů, dle vymezení vnitrostátních právních předpisů každého členského státu.[4] Tato směrnice není vztažena na obsah elektronických sdělení pouze na provozní a lokalizační a jiné související údaje, jež jsou nezbytné k identifikaci právnické a fyzické osoby jako účastníka, popřípadě registrovaného uživatele. [5] I nadále mají členské státy povinnost zajistit, a to bez nahrazení přijatých předpisů v souladu se směrnicí 95/46/ES a směrnicí 2002/58/ES dodržet zásady bezpečnosti dat jako je kvalita, technická a organizační opatření před náhodným či neoprávněným zničením, ztrátou a stejně tak pozměněním, nepovoleným i neoprávněným uchováním, popřípadě zpracování, neoprávněným přístupem a v neposlední řadě zveřejněním. Dále je nezbytné dodržet přístup k datům jenom oprávněných osob a po uplynutí doby účelu uchování dat všechny tyto údaje zničit, kromě údajů, u nichž bylo přistoupeno k uchování a byla řádně zajištěna.[6]

3.1.2 Platná právní úprava ochrany dat a informací v ČR

Zákon o ochraně osobních údajů č. 101/2000 Sb. a o změně některých zákonů, ve znění účinném od 6. října 2016 ustanovuje § 1 a § 3 vymezení rozsahu a obsahu právní úpravy zákona. „Tento zákon v souladu s právem Evropských společenství,[7] mezinárodními smlouvami, kterými je Česká republika vázána,[8] a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních

[4] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, čl.1, odst. 1

[5] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, čl.1, odst. 2

[6] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, čl. 7

[7] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

[8] Úmluva o ochraně osob se zřetelem na autorizované zpracování osobních dat č. 108, vyhlášená pod č. 115/2001 Sb.m.s.

údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.“[9] Tento právní předpis stanovuje cíle a prostředky, jimiž bude dosaženo nejen naplnění práva každého na ochranu před protiprávním zásahem do soukromí, ale zároveň je tím upraveno i právo a povinnosti při zpracování těchto údajů.

„Tento zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby.“[10] Z důvodu využívání zpracování osobních údajů ať už v oblasti sociální, hospodářské či společenské sféry bylo nutné vymezit okruh subjektů, u nichž je nezbytné, aby se těmito podmínkami řídili. Dle taxativního výčtu se zde v podstatě nachází každý subjekt, jež shromažďuje a dále zpracovává údaje, jež je možné na základě jejich povahy označit jako osobní údaje. „Tento zákon se vztahuje na veškeré zpracování osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky.“[11] Tato část působnosti zákona o ochraně osobních údajů vymezuje deklaraci zásad zpracování nikoliv prostředky a způsob, jímž je zpracování provedeno. Z hlediska historických souvislostí se jednalo o technologický cíl vývoje zaměřující se na vyhledání a zpracovávání informací. V současnosti je běžné, že všechny tyto etapy operací probíhají technickými prostředky kromě obvyklé metody pořizování a shromažďování osobních údajů přímo od subjektů na základě tradičního způsobu osobní komunikace, je zpracování zcela automatizováno. „S ohledem na charakter, efektivitu a rychlost automatizovaného zpracování přináší tento způsob provádění příslušných zpracovatelských operací nepochybně větší riziko zneužití osobních údajů, a to jak úmyslného (vyhledávání, třídění, porovnávání apod. činěné v počítačové databázi je několikanásobně rychlejší než stejná činnost v papírové kartotéce), tak i nedbalostního (lze mnohem snáze ztratit, zapomenout nebo i odcizit záznamové zařízení s tisíci osobních údajů než stejné množství osobních údajů vedených v listinné podobě).“[12] Z tohoto důvodu se první právní ustanovení, jímž byla Úmluva 108, týkala pouze automatizovaného zpracování osobních dat, což se prokázalo jako nedostatečné, neboť umožňovalo některým zpracovatelským subjektům v některých případech zpracování

[9] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 1

[10] § 3 odst. 1 zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016

[11] § 3 odst. 2 zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016

[12] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 15 a 16

se vyhnout této právní regulaci použitím neautomatizovaného zpracování. V současnosti je spíše možné setkání s kombinovaným způsobem zpracování u osobních údajů, popřípadě s převládajícím technologickým zpracováním, kdy lidský faktor funguje spíše jako kontrolní jednotka tohoto procesu. „Automatizované zpracování tedy zjednodušeně znamená, že pro zpracování osobních údajů jsou použity prostředky výpočetní techniky, případně jiné technické prostředky (kamera, videorekordér, magnetofon apod.).“[13] Za zpracování jinými prostředky naopak můžeme považovat jakékoliv manuální zpracování jako je ruční třídění, dále ukládání do kartotéky či registratury. S ohledem na způsob zpracování bude správce či zpracovatel volit zabezpečení tzn., jaké použije standardy a úrovně zabezpečení ochrany osobních údajů subjektů.

„Tento zákon se dále vztahuje na zpracování osobních údajů, jestliže se právní řád České republiky použije přednostně na základě mezinárodního práva veřejného, i když správce není usazen na území České republiky, jestliže správce, který je usazen mimo území Evropské unie; v tomto případě je správce povinen zmocnit postupem podle § 6 na území České republiky zpracovatele. Jestliže zpracování provádí správce prostřednictvím svých organizačních jednotek umístěných na území Evropské unie, musí zajistit, že tyto organizační jednotky budou zpracovávat osobní údaje v souladu s národním právem příslušného členského státu Evropské unie.“[14] Až v rámci rozsáhlejší novelizace zákona č. 439/2004 Sb. byla do legislativy vložena úprava pro ochranu osobních údajů, jež je prováděna správci sídlící mino území České republiky i Evropské unie. Do té doby nebyla tato situace zákonem upravována pouze Směrnice 95/46/ES článkem 4 požadovala zajištění uplatnění pravidel i na zpracování s mezinárodními prvky. „Právní úprava obsažená v § 3 odst. 5 písm. a) a b) OchOsÚ vychází z požadavku na zajištění stejné míry ochrany všem údajům zpracovávaným na území Evropské unie anebo dat odsud pocházejících bez ohledu na faktickou lokalizaci správce (viz recitál 20 Směrnice 95/46/ES) a jejím účelem tedy je zajištění odpovídající ochrany osobních údajů a umožnění řádného výkonu práv subjektů údajů i vůči správcům dat sídlícím mimo území EU.“[15] Naopak v případě absence takových institutů by pravděpodobně mohlo docházet v souvislosti se spravováním dat správci

[13] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 17

[14] § 3 odst. 5 zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016

[15] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 27

ze třetích zemí popřípadě migrací správců do těchto lokalit s částečnou nebo žádnou úpravou k znatelnému snížení hladiny ochrany osobních údajů z pohledu evropského prostoru. Zároveň tím je vyjádřen základní princip Evropské unie založený na spolupráci, a to zvláště o volném pohybu osobních dat uvnitř Evropské unie. To znamená, pokud je správce osobních údajů usídlený ve státě Evropské unie, může zpracovávat tyto údaje v jakémkoliv členském státě, a to bez jakéhokoliv administrativního omezení.[16]

3.2 Vymezení údajů

3.2.1 Osobní údaje

Osobní údaj je možné definovat jako jakoukoliv informaci, jež se týká určeného nebo určitelného subjektu. Lidé se často domnívají, že pod pojmem osobní údaj se skrývá pouze identifikační údaj, jež je doložený nějakým úředním dokumentem či záznamem. I v případě konkrétních údajů jako rodné číslo, datum narození atd. dochází často k mylné domněnce, že pouze v některých případech a okolnostech se jedná o osobní údaj. „Definice užitá v zákoně o ochraně osobních údajů se omezuje na vymezení vztahu údaje(ů) k tomu, o kom vypovídá, tj. subjektu údajů. Z tohoto úhle pohledu a při aplikaci zákona v praxi vyjadřuje osobní údaj vždy vztah mezi reálnou fyzickou osobou a hodnotou údaje. Zákonná definice se však vůbec nezabývá tím, co to je „údaj“.“[17] Obecně je brán termín údaj v právní úpravě ČR i v zahraničních právních předpisech téměř jako synonymum slova informace. „Pro údaje je příznačná vysoká míra normalizace, projevující se v řadě případů formalizovanou formou prezentace, obvyklé je použití tabulek nebo formulářů i mimo prostředky moderních informačních technologií.“[18] Výraz údaj je užívám v souvislosti s listinnými dokumenty, naopak při elektronickém zpracování jsou údaje nazývány jako data. Osobním údajem je tedy jakákoliv informace týkající se konkrétní osoby, na jejímž základě je možné získat obrázek o konkrétní osobě. To znamená, že za osobní údaj je možné brát každý údaj, jež je uveden do vztahu k nějaké fyzické osobě, čímž je přiřazen do vztahu subjektu údajů. Pro zjednodušení a správného pochopení pojmu

[16] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 27
[17] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 18
[18] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 19

osobní údaj se rozumí, že: „osobním údajem je jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifický pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“[19] U osobních údajů je dle zákona apelováno na jejich správnost, pravdivost a hlavně přesnost, ale Směrnice 95/46/ES vyžaduje navíc u všech členských států Evropské unie, aby osobní údaje byly přesné a pokud je to možné hlavně aktualizované.

3.2.2 Identifikační údaje

Údaje u fyzických osob

Identifikační údaje u fyzických osob jsou údaje, jež jsou nejen universálně využitelné, ale hlavně universálně využívány. Klíčovým pojmem právní úpravy na ochranu osobních údajů je z podstaty osobní údaj fyzických osob. Pro obyvatele České republiky jsou základními identifikačními údaji jméno popřípadě jména a příjmení, datum a místo narození, rodné číslo, číslo občanského průkazu i cestovního dokladu, státní občanství, adresa trvalého bydliště a jiná méně významná data.[20] „Tyto jsou člověku přiděleny v zásadě volním aktem, na rozdíl od základních údajů, které jsou zjištěny a jako jednou zjištěné v souladu s existující skutečností předepsaným způsobem, tj. převážně úředně zaznamenány.“[21] Vzhledem k technologicky vyspělé společnosti s rozvojem elektronických a jiných médií není možné omezit osobní údaj striktně jen například na jméno, rodné číslo a adresu, ale z tohoto důvodu je třeba považovat za osobní údaj i číslo mobilního telefonu určité fyzické osoby i v případě dočasného používání. Na základě telefonního čísla je subjekt nejen dosažitelný, ale i dalším způsobem určitelný, a to bez jakékoliv další znalosti osobních údajů. Lze shrnout, že každé vyjádření osobní povahy, jež je možné přiřadit ke konkrétní osobě, je v podstatě osobním údajem. Každopádně osobní údaje mohou být informace nezávislé na osobnosti jedince.

[19] § 4 Zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016

[20] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 53

[21] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 53

Jméno a příjmení

„Fyzická osoba, které byl matričním úřadem vydán matriční doklad, má povinnost užívat v úředním styku jméno, popřípadě jména, která jsou uvedena na tomto matričním dokladu“[22] Jménem je v tomto případě rozuměno osobní jméno subjektu dle občanského zákoníku. „Jméno a příjmení upravuje zákon č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů, ve znění pozdějších předpisů. Používání jména a příjmení, je právem každého občana. Je to ale i jeho povinnost před orgány veřejné moci.“[23] U těchto dvou údajů pro základní identifikaci je právo na ochranu všude tam, kde jsou používány ve spojení s jinými osobními údaji privátního charakteru. Toto právo na ochranu neplatí v případě, kdy je jméno a příjmení spojeno s aktivitami veřejného charakteru tzn. staneme-li se součástí kolektivu, v zaměstnání, politické strany, anebo sportovního klubu, pak tyto osobní údaje slouží pro vnitřní komunikaci v daném kolektivu a podle určitých zásad i pro komunikaci s veřejností či úřady.

Datum a místo narození

„Datum a místo narození jsou identifikační osobní údaje, které jsou subjektu údajů přiřazovány vlastně jako transakční údaje.[24] Oba údaje jsou dané a nelze je měnit, pouze u místa narození může časem dojít ke změně označení. Tyto údaje jsou součástí zápisu do rodného listu při narození dítěte.[25] „Jako identifikační údaje je upravuje také zákon č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů, ve znění pozdějších předpisů [§ 14 odst. 1 písm. b), c) a § 29]. Den, měsíc a rok narození se zapisují do matriční knihy narození a společně s místem narození také do rodného listu.[26] Tyto údaje společně se jménem a příjmením i popřípadě s adresou jsou používány při určování totožnosti. Výhodou těchto údajů je konstantnost neboli neměnnost po celý život.

[22] § 61 odst. 1 Zákon č. 301/2000 Sb.Zákon o matrikách, jménu a příjmení a o změně některých souvisejících zákonů
[23] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 54
[24] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 58
[25] § 29 zákon č. 301/2000 Sb. Zákon o matrikách, jménu a příjmení a o změně některých souvisejících zákonů
[26] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 58

Rodné číslo

„Problematiku rodných čísel upravuje zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů (dále jen „zákon o evidenci obyvatel“)“[27] Rodné je určováno Ministerstvem vnitra, jedná se o desetimístné číslo, jež musí být beze zbytku dělitelné jedenácti. „V informačním systému je rodné číslo identifikátorem fyzické osoby, která splňuje podmínky pro jeho přidělení podle tohoto zákona.“[28] Toto číslo je neměnným a jednoznačným identifikačním údajem fyzické osoby a zároveň je i osobním údajem. Každá fyzická osoba má přiděleno pouze jedno rodné číslo. „Rodné číslo je desetimístné číslo, které je dělitelné jedenácti beze zbytku. První dvojčíslí vyjadřuje poslední dvě číslice roku narození, druhé dvojčíslí vyjadřuje měsíc narození, u žen zvýšené o 50, třetí dvojčíslí vyjadřuje den narození. Čtyřmístná koncovka je rozlišujícím znakem fyzických osob narozených v tomtéž kalendářním dnu.“[29] Na základě současné úpravy má desetimístné rodné číslo předepsanou strukturu, kdy po šestí číslech navazuje lomítko a následuje poslední čtyřčíslí, které odlišuje osoby narozené ve stejný den. V současné době bylo upuštěno od přidělování rodných čísel s čtyřmístnou nulovou koncovkou. Kromě automatického přidělení rodného čísla při narození či osvojení nezletilé osoby, jsou dále rodná čísla přidělována nejen osobě, jež dosud rodné číslo neměla, tak i cizinci s uděleným povolením k pobytu včetně studia na vysoké škole či při ochraně formou azylu. Rodné číslo je vydáváno matričním úřadem osobám narozeným na území České republiky a občanům narozeným v zahraničí jsou přidělována rodná čísla zvláštní matrikou. V ostatních případech jako je již zmíněna ochrana formou azylu, povolení k pobytu atd. jsou přidělována rodná čísla Ministerstvem vnitra České republiky.

„Využíváním rodných čísel jejich shromažďování, vedení nebo zpracování jiným způsobem.“[30] Využíváním u rodného čísla se dle zákona rozumí jeho shromažďování nebo jiné zpracování. I na tento identifikátor se vztahuje zákona na ochranu osobních údajů, neboť mezi zpracováním osobních údajů a využívání rodného čísla není v podstatě rozdíl.

[27] Ministerstvo vnitra České republiky: Rodné číslo [online 2017] Odbor správních činností, 19. února 2016 [cit. 26.2.2017] Dostupné z: http://www.mvcr.cz/clanek/rady-a-sluzby-dokumenty-rodne-cislo.aspx
[28] § 13 zákon 133/2000 Sb., o evidenci obyvatel
[29] § 13 zákon 133/2000 Sb., o evidenci obyvatel
[30] § 13a zákon 133/2000 Sb., o evidenci obyvatel

Další osobní identifikátor – číslo občanského průkazu a cestovního dokladu

Jsou dva doklady, jejichž číslo dokladu plní po určitou dobu od vydání funkci identifikačního čísla fyzické osoby, a to občanský průkaz a cestovní doklad. „Občanský průkaz je povinen mít občan České republiky, který dosáhl věku 15 let a má trvalý pobyt na území České republiky. Občanský průkaz může mít i občan, jehož svéprávnost byla omezena.“[31] Doklad je vydáván s určitou časovou platností. „Číslo občanského průkazu jako osobní údaj upravuje zákon č. 328/1999 Sb., o občanských průkazech, v § 3 odst. 2 písm. b.). Podle tohoto čísla občanského lze určit osoby, kterým byl vydán.“[32] Za pomocí čísla dokladu lez identifikovat osoby stejně jako na základě rodného čísla, ale v tomto případě je identifikace možná pouze u osob starších 15 let.

Cestovní doklad neboli cestovní pas je vydáván pouze na základě žádosti. „Občan nepodává žádost o vydání cestovního pasu na vyplněném úředním tiskopisu, pouze předloží doklady potřebné k vydání cestovního pasu, např. občanský průkaz. Občan nepředkládá fotografii, protože fotografii pořizuje příslušný úřad při podání žádosti – proto se občan musí k němu osobně dostavit.“[33] Cestovní doklad je vydáván na určitou časově omezenou dobu a není vymezena věková hranice pro jeho získání. „Číslo cestovního dokladu upravuje zákon č. 329/1999 Sb., o cestovních dokladech, v § 6 odst. 3 písm. b). Také číslo cestovního dokladu je možné použít obdobně jako číslo občanského průkazu pro identifikaci např. při ubytování.“[34] I v tomto případě se jedná o číslo jedinečné, a tudíž je na jeho základě dle příslušné evidence možné vyhledat osoby, jimž byl tento cestovní doklad vydán.

[31] Ministerstvo vnitra České republiky: Rodné číslo [online 2017] Odbor správních činností, 13. ledna 2017 [cit. 26.2.2017] Dostupné z: http://www.mvcr.cz/clanek/osobni-doklady-642319.aspx?q=Y2hudW09NA%3d%3d

[32] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 69

[33] Ministerstvo vnitra České republiky: Rodné číslo [online 2017] Odbor správních činností, 13. ledna 2017 [cit. 26.2.2017] Dostupné z: http://www.mvcr.cz/clanek/osobni-doklady-642319.aspx?q=Y2hudW09NA%3d%3d

[34] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 69

3.2.3 Citlivé údaje

„Citlivé údaje je možné zpracovávat, jen jestliže: subjekt údajů dal ke zpracování výslovný souhlas. Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Existenci souhlasu subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování.“[35] Správce před žádostí o souhlas je povinen neprodleně informovat subjekt pro jaký účel souhlas žádá a jaká má subjekt práva.

„Citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.“[36] Výčet citlivých údajů je úplný a jiné údaje nemají povahu citlivých údajů. „Důmyslná argumentace, proč některý osobní údaj na první pohled vykazující charakteristiky citlivého osobního údaje není považován za citlivý osobní údaj, je vždy motivována snahou vyhnout se splnění přísnějších podmínek stanovených zákonem o ochraně osobních údajů.“[37] Může být totiž zpochybňováno to, jestli určitý údaj skutečně vypovídá o tom, co by mohlo být jako citlivý údaj zneužitelné. Citlivý údaj je neveřejná informace, u níž je nezbytná ochrana, neb zveřejnění této informace, použití, změna, ztráta nebo i zničení by mohlo způsobit škodu osobě, které se informace týká. Respektive k tomu, aby bylo možné údaj označit jako citlivý, je nutné, aby splňoval nejenom znaky požadované pro osobní údaje, ale současně je nezbytné, aby bylo možno na jeho základě určit národnost, rasový původ, i členství v politické straně a další údaje o subjektu tzn. identifikovat subjekt. „Za citlivé jsou v ochraně osobních údajů považovány takové osobní údaje, které mohou být využity k diskriminaci subjektu údajů.“[38] Pokud údaj obsahuje nejen citlivé ale i osobní údaje je nutné při jeho zpracování postupovat podle ustanovení o citlivých osobních údajích.

[35] § 9 odst. 1 Zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016

[36] Viz § 4 Zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016

[37] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 80

[38] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 81

3.2.4 Práva a povinnosti správce osobních údajů

Správce osobních údajů je dle zákona o ochraně osobních údajů každý subjekt, jemuž zákon ukládá povinnost zpracovávat osobní údaje. Zároveň mu zákon ukládá povinnost, jak s těmito údaji pracovat a naložit.

„Správce je povinen stanovit účel, k němuž mají být osobní údaje zpracovány, stanovit prostředky a způsob zpracování osobních údajů, zpracovat pouze přesné osobní údaje, které získal v souladu s tímto zákonem. Je-li to nezbytné, osobní údaje aktualizuje. Zjistí-li správce, že jím zpracované osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje opraví nebo doplní, jinak osobní údaj zlikviduje.“[39] Poskytování osobních údajů by mělo být dobrovolné. Správce je tedy povinen stanovit za jakým účelem budou tyto osobní údaje zpracovávány. Tento účel neboli cíl je správcem popsán i odůvodněn. Podle zákona o ochraně osobních údajů je toto stanovení účelu pro zpracování osobních údajů zásadní kategorií pro posuzování plnění povinností. Za účelem uzavření účastnické smlouvy a plnění závazků (například u mobilního operátora) jsou některé osobní údaje nezbytné nejen pro poskytování služeb a produktů.[40] Pod pojmem zpracování osobních údajů se zejména rozumí shromažďování, ukládání na nosiče, úprava nebo pozměňování v případě aktualizace dat, třídění nebo kombinování, blokování i likvidace v souladu se Směrnicí 95/46/ES. Pokud se jedná o nepřesné osobní údaje, je nutné je označit. Dále je správcova povinnost bez zbytečného odkladu informovat všechny příjemce o blokování, opravě, doplnění nebo likvidaci osobních údajů.

„Správce je povinen shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu, uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů a osobní údaje anonymizovat, jakmile je to možné.“[41] Shromažďování dat správcem je systematický postup,

[39] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 99
[40] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 202
[41] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 99

popřípadě soubor postupů získávání osobních údajů, ať už pro jejich okamžité uložení na nosič informací nebo jejich pozdější zpracování. Nicméně každé získání osobního údaje či dokumentu s osobními údaji nemůže být bráno jako shromažďování. Je nezbytné rozlišení mezi třemi pravděpodobnými způsoby získání osobních údajů, což má pro následné zacházení s osobními daty velký význam. Mezi tyto tři způsoby patří postupné nashromáždění, dále řešení případu nebo popis události či jevu při jednorázovém okamžitém použití a jako poslední způsob je získání osobních dat bez jakéhokoliv záměru či vynaloženého úsilí, a to jako nahodilé získání osobních údajů třeba přijetí vizitky. Správce je povinen určit dobu uchování dat pro účely archivnictví po uplynutí doby nezbytné k jejich zpracovávání, subjekt muže po tuto dobu kdykoliv odvolat svůj souhlas. V případě, že souhlas není poskytnuta nebo poskytovatel svůj souhlas odvolá je správce povinen zpracování ukončit a údaje zlikvidovat.

„Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat, jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce, jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů.“[42] Správce osobních údajů je povinen zvolit způsob a prostředky, jež jsou mu přičitatelné. Též správce může stanovit svého zpracovatele, pokud nebude data zpracovávat sám.

„Zpracovatelem je pak od správce odlišný subjekt, který zpracovává osobní údaje na základě zvláštního zákona nebo pověření správce.“[43] Toto jeho rozhodnutí může být provedeno zpracovatelem s jeho vědomím a následným schválením, popřípadě je provedeno správcem samotným. „Pokud zmocnění nevyplývá z právního předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.“[44] Zpracovatel je oprávněn zpracovávat osobní údaje subjektů pro správce komplexně, ale jeho oprávnění se vztahuje na některé dílčí části, kdy tato úprava je nedílnou součástí smlouvy mezi správcem

[42] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 99 a 100

[43] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 175

[44] Viz § 6 Zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016

a zpracovatelem. V té musí být uvedeno v jakém rozsahu, dále za jakým účelem, a zvláště i na jakou dobu je smlouva uzavírána. Též musí obsahovat veškeré záruky zpracovatele včetně technického i organizačního zabezpečení ochrany osobních údajů subjektů. Náležitosti této zpracovatelské smlouvy a úpravu vztahu mezi správcem a zpracovatelem upravuje zákon 101/2000 Sb. o ochraně osobních údajů § 6. Nicméně v případě, že zmocnění vyplývá ze zvláštního zákona zpracování osobních údajů zpracovatelem, není třeba mít uzavřenou za těchto okolností smlouvu. Povinnosti zpracovatele jsou v podstatě přiměřené povinnostem správce.[45] Základní prvek, jež odlišuje správce od zpracovatele je povinnost stanovení účelu zpracování osobních údajů, což je výhradně oprávněn stanovit pouze správce. Zpracovatel se však může podílet stejnou i větší měrou než správce na plnění povinností spjatých s tímto zpracováním. Lze tedy jednoznačně shrnout, že v kontextu tohoto zákona byla zákonodárcem stanovena odpovědnost zpracovatele poměrně přísně v podstatě ve stejné velikosti jako správci osobních údajů. „Jestliže zpracovatel zjistí, že správce porušuje povinnosti stanovené tímto zákonem, je povinen jej na to neprodleně upozornit a ukončit zpracování osobních údajů. Pokud tak neučiní, odpovídá za škodu, která subjektu údajů vznikla, společně a nerozdílně se správcem údajů. Tím není dotčena jeho odpovědnost podle tohoto zákona.“[46] Tímto je posílena odpovědnost zpracovatele, neboť mu ukládá povinnost při zjištění porušení povinnosti, jež je stanovena zákonem správci, neprodleně správce na tuto skutečnost upozornit a případně předmětné zpracování okamžitě ukončit. Ukončit v tomto případě neznamená zlikvidovat, ale spíše ono zpracování pozastavit a vyčkat na reakci správce, pro něhož jsou data zpracovávána.[47]

Kromě informační povinnosti správce vůči Úřadu na ochranu osobních údajů o zamýšleném zpracování dat subjektů je správce též povinen sdělit Úřadu plánovaný způsob a zvolené prostředky. Definovat způsob a prostředky tohoto zpracování je nepochybně neoddělitelnou součástí rozhodnutí správce. „Výslovné zakotvení povinnosti stanovit prostředky a způsob zpracování v zákoně o ochraně osobních údajů nepochybně přispívá ke snazší vymahatelnosti této povinnosti a současně zvyšuje instruktivnost zákona

[45] Viz § 7 Zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016

[46] Viz § 8 Zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016

[47] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 180

o ochraně osobních údajů ve vztahu k jeho adresátům.“[48] Rozdíl mezi prostředky a způsobem zpracování není až tak výrazný. Pojem prostředky zpracování lze definovat jako technická a technologická zařízení tzn.: jak je zpracování provedeno, zda informačním systémem nebo připraveným dotazníkem, formulářem či jiným způsobem. V případě pojmu způsobu zpracování se jedná o určitou metodu vyhodnocení těchto získaných dat, a to je zejména základní rozlišení na manuální, automatizované i kombinované zpracování. Mezi manuální prostředky zpracování je možné zařadit nejrůznější formuláře. V případě elektronické podoby dat se jedná o automatizované standartní zpracování s využitím výpočetní techniky.

„Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může a) požádat správce nebo zpracovatele o vysvětlení, b) požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav. Zejména se může jednat o blokování, provedení opravy, doplnění nebo likvidaci osobních údajů.“[49] Pokud se subjekt, jehož se osobní údaje týkají, domnívá nebo zjistí, že nejsou tyto údaje zpracovány s ochranou jeho soukromého a osobního života popřípadě v rozporu se zákonem, může požádat správce anebo zpracovatele, nejen o vysvětlení, ale hlavně může požádat o nápravu vzniklého stavu. Odstranění neboli náprava daného stavu může proběhnout blokací, opravou údajů, doplněním do správného stavu nebo likvidací osobních údajů, a to zvláště pokud se jedná o nepřesné osobní údaje. Subjekt si sám zvolí, jakým procesem dojde k nápravě.

„Došlo-li při zpracování osobních údajů k porušení povinností uložených zákonem u správce nebo zpracovatele, odpovídají za ně společně a nerozdílně.“[50] Jedná se tedy o jakési solidární ustanovení. Je pouze na poškozeném subjektu, kterého ze škůdců zvolí, zda správce či zpracovatele a bude se na něm domáhat své pohledávky. V případě, že jeden ze škůdců tento závazek vůči subjektu splatil, závazek všech ostatních tímto aktem zaniká.

[48] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 109

[49] Viz § 21 Zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016

[50] Viz § 21 Zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016

3.2.5. Povinnost správce likvidace osobních údajů

Likvidací osobních dat je v podstatě uzavírán proces jejich zpracování a jedná se tak o jejich poslední etapu, čímž je rozuměno, že po této transakci nebudou již data existovat a nelze je žádným technickým úkonem obnovit. Při pominutí účelu, pro jaký byla osobní data neboli údaje spravována správcem, popřípadě na základě žádosti subjektu, jehož se tyto data týkají je správce povinen v obou případech tyto informace zlikvidovat. Za provedení této likvidace je zodpovědným subjektem osoba, jež o zpracování těchto informací rozhodla, určila účel i prostředky. Celou transakci až po definitivní znehodnocení neboli likvidaci dat, popřípadě nosičů těchto dat, musí mít správce pod kontrolou, a to i v případě, že touto likvidací pověří zpracovatele.

„Zvláštní zákon stanoví výjimky týkající se uchování osobních údajů pro účely archivnictví a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení.“[51] Zvláště se jedná o dvě výjimky, kdy je nutné osobní údaje uchovat na základě zvláštního zákona, a tudíž nepodléhají likvidaci, ať už se jedná o účel archivnictví, anebo z důvodu uplatnění v občanskoprávním, trestním i správním řízení. U první výjimky se jedná o uchování osobních údajů výlučně pro archivnictví, a to i bez souhlasu subjektu, k němuž se tyto osobní údaje vztahují. „Druhá výjimka se vztahuje na případy, kdy správce zpracovávané osobní údaje dále potřebuje pro odlišný účel, než pro který je původně získal a zpracovával, a to konkrétně pro uplatnění svých práv v občanském, správním nebo trestním řízení.“[52] Správce je povinen zajistit i za těchto okolností náležitou a zákonem uloženou ochranu osobních údajů, byť původní účel a zcela odlišný již pominul. Ani v tomto případě výjimky pro likvidaci osobních údajů není doba držení těchto osobních údajů neomezená a měla by být odpovědna době promlčení upravené zvláštními právními předpisy.

3.2.6. Dozorčí orgán pro ochranu osobních údajů

V České republice se jedná hlavně o nový dozorový orgán Úřad pro ochranu osobních údajů, který je označován jako nezávislý správní orgán, jež splňuje požadavky dle Úmluvy č. 108 a článku 28 směrnice 95/46/ES pro dozorové orgány členských států EU to znamená, že se jedná o nezávislý orgán, jež nepodléhá ani ministerstvu ani jinému státnímu orgánu. „Činnost

[51] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 274
[52] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 277

Úřadu je vymezena ZoOU a některými dalšími zákony.“[53] Hlavní náplní tohoto dozorčího orgánu je dozor nad dodržováním zákonem stanovených povinností při zpracování osobních dat, nedílnou součástí je i přijímání stížností na porušení zákona a podnětů od subjektů. Současně však poskytuje konzultace a rady se zaměřením na ochranu osobních údajů. „Nezávislost ÚOOÚ je založena dále tím, že jeho předseda a sedm inspektorů jsou jmenováni a odvoláváni prezidentem republiky na návrh Senátu Parlamentu České republiky.“[54] Předseda pro tento úřad bývá jmenován na dobu pěti let, nejvýše může být jmenován na dvě po sobě jdoucí období, to znamená maximálně na dobu deseti let. Předseda na této pozici nejen řídí úřad, ale zároveň i zastupuje Českou republiku v Poradním výboru Rady Evropy k Úmluvě č. 108 a v Pracovní skupině Evropské unie podle článku 29 Evropské unie, nedílnou součástí je zasedání na mezinárodních komisařů a dále vykonává některé jmenovitě uvedené činnosti, jež jsou uvedené v ustanoveních zákona o ochraně osobních údajů. Inspektor tohoto úřadu musí být nejen občanem České republiky, ale musí i splňovat kritéria jako je způsobilost k právním úkonům, bezúhonnost, dokončené odborné vysokoškolské vzdělání a je nezbytné, aby splňoval i podmínky stanovené zvláštním právním předpisem. Jeho jmenování na tento post bývá na období deseti let a jeho jmenování do funkce je možné opakovat. „Podle zákona o ochraně osobních údajů inspektor vykonává kontrolu, řídí kontrolu, vypracovává kontrolní protokol a provádí další úkony, jež souvisejí s úkoly ÚOOÚ.“[55] Funkce inspektora je neslučitelná s funkcí ve veřejném životě, členství v politických stranách i hnutích, dále není z této pozice možné zastávat jinou placenou funkci, ani nesmí být v jiném pracovním poměru či jiné výdělečné činnosti, s výjimkou vědecké činnosti, pedagogické, literární, publicistické, umělecké činnosti a správy vlastního majetku v případě, že tato činnost nenarušuje důstojnost či nesnižuje důvěru v nezávislost a nestrannost funkce tohoto úřadu.

[53] Bartík, V., Janečková, E., Ochrana osobních údajů v životě podnikatele. 1. vydání edice právo, Nakladatelství ANAG, 2013 str. 151

[54] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 331

[55] Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, str. 331

3.3 Ochrana dat a informací se zaměřením na mobilního operátora

3.3.1 Vývoj platné právní úpravy o elektronických komunikacích

O elektronických komunikací pojednává Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů a dále některé směrnice Evropského parlamentu a Rady. „Tento zákon upravuje na základě práva Evropské unie podmínky podnikání a výkon státní správy, včetně regulace trhu, v oblasti elektronických komunikací.“[56] Pro účely tohoto zákona je nezbytné vymezení některých pojmů. „Práva a povinnosti související s ochranou osobních údajů neupravené v tomto dílu se řídí zvláštním právním předpisem.“[57] V tomto případě neupravená práva a povinnosti týkající se ochrany osobních údajů upravuje zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. „Souhlasem podle zvláštního právního předpisu[58] se pro účely tohoto dílu rozumí rovněž souhlas učiněný pomocí elektronických prostředků, zejména vyplněním elektronického formuláře na internetu.“[59] Je zákonem na ochranu osobních údajů stanoveno, že musí subjekt se zpracováním osobních údajů souhlasit, a to za určitých zákonných podmínek. „Subjekt údajů musí být při udělení souhlasu, který je pouze svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů, informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období.“[60] Správce je povinen se prokázat souhlasem se zpracováním osobních údajů subjektu po celou dobu zpracovávání, což platí i pro oblast elektronických komunikací. „Současně byla do zákona o elektronických komunikacích, s ohledem na specifika zpracování osobních údajů v této oblasti, vložena samotná právní úprava, podle které se za souhlas se zpracováním osobních údajů pro účely tohoto dílu zákona o elektronických komunikacích rozumí rovněž souhlas učiněný pomocí elektronických prostředků, tedy zejména vyplněním elektronického formuláře na internetu (zákon o ochraně osobních údajů nicméně formu souhlasu nijak

[56] Vaníček, Z., Mates, P., Nielsen, T.: Zákon o elektronických komunikacích. Komentář. Praha: Linde Praha a. s., 2014, str. 13

[57] § 87 zákon č. 127/2005 Sb. o elektronických komunikacích, a o změně některých souvisejících zákonů

[58] § 5 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

[59] § 87 zákon č. 127/2005 Sb. o elektronických komunikacích, a o změně některých souvisejících zákonů

[60] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 473

neupravuje, a tedy nevylučuje ani zde výslovně uvedenou možnost využití elektronického formuláře).“[61] Vzhledem k nezbytnému podpisu pro potvrzení souhlasu i u elektronických komunikacích je možné použití jiné formy souhlasu než podpisu například kliknutí na příslušnou ikonu formuláře či opětovný dvojité kliknutí na příslušnou ikonu. Potvrzení dvojitým kliknutím se používá z důvodu vyloučení možnosti mylného kliknutí – potvrzení. Stejně jako v ostatních případech je nutné, aby správce prokázal obdržení souhlasu subjektu o zpracování, kdykoliv v průběhu zpracovávání osobních údajů.

„Dozor nad dodržováním povinností při zpracování osobních údajů podle tohoto zákona vykonává Úřad pro ochranu osobních údajů podle zvláštního předpisu[62].“[63] Toto ustanovení stanovuje kompetence Úřadu pro ochranu osobních údajů dozorovat dodržování povinností při zpracovávání osobních údajů subjektů na základě zákona o elektronických komunikacích. Není možno opomenout výkon dozoru ÚOOÚ podle zvláštních předpisů, jímž je primárně zákon o ochraně osobních údajů a v této návaznosti ustanovení i zákon o státní kontrole a správní řád.

„Podnikatel poskytující veřejně dostupnou službu elektronických komunikací je povinen zajistit technicky a organizačně bezpečnost poskytované služby s ohledem na ochranu osobních údajů fyzických osob v souladu se zvláštním právním předpisem, ochranu provozních a lokalizačních údajů a důvěrnost komunikací fyzických a právnických osob při poskytování této služby; pokud je to nutné, ochranu zajistí po písemné dohodě i v součinnosti s podnikatelem zajišťujícím veřejnou komunikační síť.“[64] Jedná se o jednu z hlavních povinností podnikatele, jež poskytuje veřejně dostupnou službu a tou je zajištění technické a organizační bezpečnosti s ohledem na ochranu osobních údajů. V prostředí elektronických komunikací má ochrana osobních údajů zvláštní právní podmínky, ale současně je jejím základem i zákon o ochraně osobních údajů. „Podnikatel poskytující veřejně dostupnou službu elektronických komunikací je povinen zpracovat pro zajištění ochrany údajů a důvěrnosti komunikací podle písmene a) vnitřní technicko – organizační předpis; ochranu údajů a důvěrnost komunikací zajistí s ohledem na stávající technické

[61] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 473

[62] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

[63] § 87 zákon č. 127/2005 Sb. o elektronických komunikacích, a o změně některých souvisejících zákonů

[64] § 88 zákon č. 127/2005 Sb. o elektronických komunikacích, a o změně některých souvisejících zákonů

možnosti a na náklady potřebné k zajištění ochrany na úrovni odpovídající existujícímu riziku porušení ochrany.“[65] Předpisem uvnitř organizace je nutné stanovit základní povinnosti, jimiž podnikatel zajistí ochranu údajů a zvláště důvěrnost komunikací s ohledem na technické možnosti včetně nákladů potřebných k zajištění ochrany. Podnikatel má též povinnost informovat zákazníky o příznačném riziku porušení sítě stran bezpečnosti ochrany dat a v případě přesahu rozsahu jeho opatření proti riziku, je nezbytné účastníky informovat o všech možnostech nápravy včetně nákladů s tím souvisejících.

„V případě porušení ochrany osobních údajů fyzické osoby je povinen podnikatel poskytující veřejně dostupnou službu elektronických komunikací oznámit bez zbytečného odkladu tuto skutečnost Úřadu pro ochranu osobních údajů. Toto oznámení obsahuje popis důsledků porušení ochrany a technická ochranná opatření, která podnikatel přijal, nebo navrhuje přijmout.“[66] Očekává se, že všechny kroky, které podnikatel podnikne pro zabezpečení dat, bude možné monitorovat zvláště Úřadem na ochranu dat. V případě, že k bezpečnostnímu incidentu dojde, je hlavní zásadou přijetí přiměřeného opatření maximálně snižující dopad včetně cíle předejít obdobným zásahům do systému. „Oznamovatelem porušení ochrany osobních údajů, je pouze poskytovatel veřejně dostupných služeb elektronických komunikací, který je držitelem osvědčení vydaného Českým telekomunikačním úřadem.“[67]

3.3.2. Platná právní úprava zákona o kybernetické bezpečnosti

Legislativní úprava zákona o kybernetické bezpečnosti patří mezi nové úpravy, tzn. nový právní předpis pro oblast, jež nebyla do roku 2012 regulována. Tato regulace vstoupila v platnost zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Tento zákon byl vypracován z důvodu narůstajících využití informačních technologií, kdy se společnost stává závislá na technologiích a tím narůstá možné riziko jejího zneužití k útokům, jež pak mají rozsáhlý dopad na činnost subjektů, potažmo mohou vést i ke značným ekonomickým škodám celé společnosti. „Závislost společnosti a jejího fungování na informačních technologiích rapidně

[65] § 88 zákon č. 127/2005 Sb. o elektronických komunikacích, a o změně některých souvisejících zákonů

[66] § 88 zákon č. 127/2005 Sb. o elektronických komunikacích, a o změně některých souvisejících zákonů

[67] [67] Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, str. 478

narůstá, a to ve všech oblastech (nejedná se pouze o služby informační společnosti, jako je internetový obchod, ale i o fungování informačních systémů na jejichž správné funkci je závislá celá řada základních služeb, jako například řízení dopravy, přenos energií, výkon veřejné moci apod.).“[68] Vzhledem k tomu, že kybernetický prostor nezná hranic, je kvalitní ochrana informačních technologií důležitým celosvětovým trendem.

„Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.“[69] Pod pojmem kybernetická bezpečnost rozumíme souhrn všech prostředků, jež směřuje a zajišťuje ochranu kompletního kybernetického prostoru. „Tento zákon zapracovává příslušné předpisy Evropské unie a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.“[70] V ČR je nejdůležitějším orgánem Národní bezpečnostní úřad, kdy tento úřad je nejdůležitějším vykonavatelem státní správy, jež zajišťuje kybernetickou bezpečnost v součinnosti s národním a vládním dohledovým pracovištěm CERT.

„V tomto zákoně se rozumí kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“[71] Kybernetickým prostorem je myšleno digitální prostředí, což je tak zvaně virtuální prostor uměle vytvořený člověkem. V tomto prostředí dochází k výměně a zpracování informací, jež jsou tvořeny elektronickými komunikacemi, službami a informačními systémy. Virtuální prostředí umožňuje uchování, sdílení a výměnu informací i jejich možné zpracování. Síť elektronických komunikací je přenosový systém, kterým je umožněn přenos signálu, a to buď rádiový, elektromagnetický či optický. „Síť elektronických komunikací zahrnuje družicové sítě, pevné sítě s komutací okruhů nebo paketů, mobilní zemské sítě, sítě pro rozvod elektrické energie, sítě pro rozhlasové

[68] Maisner, M., Vlachová, B.: Zákon o kybernetické bezpečnosti. Komentář, vydání Praha: Wolters Kluwer, a.s., 2015, str. 1
[69] §1 zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. A zákona č. 205/2017 Sb.
[70] §1 zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. A zákona č. 205/2017 Sb
[71] §2 zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. A zákona č. 205/2017 Sb.

a televizní vysílání a sítě kabelové televize.“[72] Služba elektronických komunikací je poskytována subjektem převážně za úplatu, jež využívají převážně sítí elektronických komunikací.

„Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací.“[73] Tímto ustanovením jsou vymezeny nejen orgány i osoby, ale i subjekt, jež se může stát poskytovatelem služby elektronických komunikací i zajišťování sítí elektronických komunikací, jímž tento zákon ukládá povinnosti v oblasti kybernetické bezpečnosti. „Podnikat v elektronických komunikacích na našem území mohou fyzické a právnické osoby, které splňují obecné podmínky dle zákona o elektronických komunikací.“[74] Mezi základní podmínky patří dosažení věku 18 let, způsobilost k právním úkonům u fyzických osob i bezúhonnost.

„Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací [75] v kybernetickém prostoru.“[76] V tomto případě opatření je chápáno jako úkon, jež zajišťuje bezpečnost informací včetně dostupnosti, spolehlivosti všech služeb v sítí elektronických komunikací v kybernetickém prostoru. Nicméně hlavní povinnost bezpečnostního opatření je uložena správcům významného informačního systému, a-nebo kritické informační infrastruktury[77]. „Poskytovatel digitální služby je povinen zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a in formační systémy, které využívá v souvislosti se zajišťováním své služby, přičemž tato bezpečnostní opatření zohledňují zajištění bezpečnosti informací, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností,

[72] Maisner, M., Vlachová, B.: Zákon o kybernetické bezpečnosti. Komentář, vydání Praha: Wolters Kluwer, a.s., 2015, str. 66

[73] §3 zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb.

[74] Maisner, M., Vlachová, B.: Zákon o kybernetické bezpečnosti. Komentář, vydání Praha: Wolters Kluwer, a.s., 2015, str. 75

[75] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

[76] §4 odst. 1 zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb

[77] Kritická informační infrastruktura je souhrn prvků či systémů kritické infrastruktury v odvětví informačního systému v oblasti kybernetické bezpečnosti.

monitorování, audit, testování a soulad s mezinárodními předpisy.“[78] Jsou rozlišeny dvě skupiny bezpečnostní opatření. První skupina bezpečnostního opatření je označována jako organizační a druhá jako technické opatření. Pod pojmem organizační opatření je uvedeno:

„a) systém řízení bezpečnosti informací,

b) řízení rizik,

c) bezpečnostní politika,

d) organizační bezpečnost,

e) stanovení bezpečnostních požadavků pro dodavatele,

f) řízení aktiv,

g) bezpečnost lidských zdrojů,

h) řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,

i) řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,

j) akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,

k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

l) řízení kontinuity činností a

m) kontrola a audit kritické informační infrastruktury a významných informačních systémů.“[79]

Mezi organizační opatření je zahrnuta nejen povinnost vyhotovovat plány, ale i uplatnit organizační, řídící a samozřejmě i kontrolní postupy procesů spravovanými osobami i orgány, jež souvisí s provozem komunikačních a informačních komplexů.

[78] §4 odst. 3 zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb.

[79] §5 odst. 2 zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb.

Pod pojmem technické opatření je uvedeno:

„a) fyzická bezpečnost,

b) nástroj pro ochranu integrity komunikačních sítí,

c) nástroj pro ověřování identity uživatelů,

d) nástroj pro nařízení přístupových oprávnění,

e) nástroj pro ochranu před škodlivým kódem,

f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,

g) nástroj pro detekci kybernetických bezpečnostních událostí,

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,

i) aplikační bezpečnost,

j) kryptografické prostředky,

k) nástroj pro zajišťování úrovně dostupnosti informací a

l) bezpečnost průmyslových a řídících systémů.“[80]

Ve složce technických opatření jsou vyspecifikovány složky řešení, jež se týkají zabezpečení komunikačních a informačních systémů včetně odhalování, posuzování a východiska kybernetických bezpečnostních incidentů a případných událostí. Mezi povinnosti zavedení bezpečnostního opatření náleží i zpracování bezpečnostní dokumentace.

„Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[81].“[82] Kybernetická bezpečnostní událost je událostí bez reálného negativního dopadu na určitý informační či komunikační systém. Jedná se o tzv. potenciální porušení či poškození bezpečnosti v informačním sektoru včetně integrity

[80] §5 odst. 3 zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb.

[81] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

[82] §7 odst. 1 zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb

sítí elektronických komunikací. „Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[83] v důsledku kybernetické bezpečnostní události.“[84] Kybernetický bezpečnostní incident je událost s dopadem na kybernetickou bezpečnost a možnými následky. Základem tohoto zákona je zajištění kybernetické bezpečnosti v České republice s důrazem na bdělost k státům celého světa. Jedním ze základů kybernetické ochrany je znemožnit využití českých komunikačních a informačních systémů k možným útokům do zahraničních subjektů a sítí.

V případě ohrožení probíhá hlášení kybernetického bezpečnostního incidentu. „Orgány a osoby uvedené v § 3 písm. b) až f) jsou povinny hlásit kybernetické bezpečnostní incidenty v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému, a to bezodkladně po jejich detekci; tím není dotčena informační povinnost podle jiného právního předpisu[85] nebo přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů[86]. V případě, že kybernetický bezpečnostní incident má významný dopad na kontinuitu poskytování základní služby, oznámí to provozovatel základní služby Úřadu[87].“[88] Osoby a orgány, které mají povinnost ohlásit veškeré kybernetické bezpečnostní incidenty, jsou určeny tímto zákonem. Tyto incidenty je nutné hlásit bez jakékoliv odkladu v případě detekce kybernetické bezpečnostní události, jež je posouzena jakožto kybernetický bezpečnostní incident. Součástí této ohlašovací povinnosti je i povinnost informovat o přijatých či zamýšlených opatření k opravě i o předpokládaném termínu odstranění příčiny. „Poskytovatel digitální služby je povinen bez zbytečného odkladu hlásit kybernetický bezpečnostní incident s významným dopadem

[83] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.
[84] §7 odst. 2 zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb.
[85] Například § 98 odst. 4 a § 99 odst. 4 zákona č. 127/2005 Sb., ve znění pozdějších předpisů.
[86] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ohraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízeni o ochraně osobních údajů).
[87] NBÚ (Národní bezpečnostní úřad) jedná se o ústřední orgán ve státní správě ČR, který uskutečňuje správu v oblasti ochrany
[88] §8 odst. 1 zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb.

na poskytování jeho služeb, pokud má přístup k informacím nezbytným pro posouzení významnosti tohoto dopadu.“[89] Naopak Úřad má povinnost vést evidenci všech těchto kybernetických útoků neboli incidentů. Podporu Úřadu tvoří národní CERT, jehož součástí bude i vládní CERT, jež bude bezprostředně reagovat na počítačové incidenty. Národní CERT musí být většinou provozován subjektem soukromého práva, který uzavře veřejnoprávní smlouvu s Národním bezpečnostním úřadem. „Vůči národnímu CERT budou poskytovatelé služeb elektronických komunikací, subjekty zajišťující sítě elektronických komunikací a subjekty zajišťující významné sítě realizovat svou zákonnou notifikační povinnost.“[90] Národní CERT má úkoly jako je posuzování zranitelnosti kybernetického prostředí a bezpečnosti, evidovat oznámení, přijímat hlášení o bezpečnostních incidentech a současně vyhodnocování těchto bezpečnostních incidentů. CERT má povinnost postupovat nestranně v plnění těchto úkolů a zároveň postupovat informace o kybernetických bezpečnostních incidentech Národnímu bezpečnostnímu úřadu. Součástí Národního bezpečnostního úřadu je vládní CERT. Úkolem vládního CERT je přijímání údajů od národního provozovatele CERT, přijímání podnětů z oblasti kybernetiky od různých subjektů, poskytuje pomoc včetně podpory. Dále stejně jako národní CERT „přijímá hlášení o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech, poskytuje součinnost při jejich řešení a poté je vyhodnocuje“[91]. Součástí úkolů vládního CERT je metodická podpora i pomoc, příjem podnětů v oblasti kybernetiky od různých subjektů, včetně příjmu „oznámení kontaktních údajů od správců informačních a komunikačních systémů kritické informační infrastruktury a správců významných informačních systémů“[92], součástí náplně je i hodnocení zranitelnosti v této oblasti.

[89] §8 odst. 2 zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb.

[90] Maisner, M., Vlachová, B.: Zákon o kybernetické bezpečnosti. Komentář, vydání Praha: Wolters Kluwer, a.s., 2015, str. 120

[91] Maisner, M., Vlachová, B.: Zákon o kybernetické bezpečnosti. Komentář, vydání Praha: Wolters Kluwer, a.s., 2015, str. 128

[92] Maisner, M., Vlachová, B.: Zákon o kybernetické bezpečnosti. Komentář, vydání Praha: Wolters Kluwer, a.s., 2015, str. 128

3.3.3. GDPR – Obecné nařízení o ochraně osobních údajů

„Rychlý technologický rozvoj a globalizace s sebou přinesly nové výzvy pro oblast ochrany osobních údajů. Rozsah shromažďování a sdílení osobních údajů významně vzrostl. Technologie umožňují jak soukromým společnostem, tak orgánům veřejné moci využívat při provádění jejich činností osobní údaje v nebývalém rozsahu.“[93] Z důvodu nedostatečné současné ochrany osobních údajů v EU došlo k vypracování obecného nařízení, které bylo schváleno a podepsáno Evropským parlamentem a Radou (EU) 27. dubna 2016 o ochraně osobních údajů na úrovni Evropské unie pod názvem General Data Protection Regulation – GDPR, jež začne platit jednotně ve všech členských státech 25. května 2018, kdy období od schválení po dobu vstoupení v platnost má být věnováno členskými státy k přípravě. V průběhu této doby je nezbytné, aby všichni zrevidovali své informační systémy včetně postupů nakládání s osobními údaji. V České republice bude tímto nařízením nahrazena současná právní úprava ochrany osobních údajů, jež je stanovena doposud platnou Směrnicí 95/46/ES a zákonem 101/2000 Sb., o ochraně osobních údajů. Vzhledem k tomu, že tato nová ucelená pravidla byla přijata pod formou nařízení, je tím stanovena přímo použitelná jednotná platnost bez jakéhokoliv přizpůsobování jiným zájmům. „GDPR se dotkne každého, kdo shromažďuje nebo zpracovává osobní údaje Evropanů, včetně společností a institucí mimo území EU, které působí na evropském trhu.“[94] Nařízení se dotkne v podstatě každého, je zaměřeno na společnosti, instituce a v neposlední řadě i jednotlivce. Dotkne se tedy všech, kteří nějakým způsobem zachází s osobními daty, ať už se jedná o data zákazníků, zaměstnanců i dodavatelů skrz veškerá odvětví. Přijetím konečného znění obecného nařízení EU očekává pevné stanovy pro ochranu údajů a zároveň o důrazné vymáhání práva.

Stávající směrnice 95/46/ES definuje osobní údaje jako veškeré informace, jež se vztahují k fyzické osobě. Mezi osobní údaje je řazeno jméno a příjmení, věk a datum narození tzn. veškeré identifikační údaje, citlivé údaje i adresní údaje včetně IP adresy. „Osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo,

[93] 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

[94] GDPR – Obecné nařízení o ochraně osobních údajů: Co je GDPR a jak bude aplikováno v Česku [online] Škorničková, E., [cit. 25.3.2017] dostupné z: https://www.gdpr.cz/gdpr/co-je-gdpr/

lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“[95] GDPR se vztahuje i na podnikající fyzické osoby, tudíž součástí osobních údajů budou i organizační údaje jako je e-mailová adresa, telefonní číslo i jiné identifikační údaje státem vydané. „Obecné nařízení věnuje speciální pozornost zpracování zvláštních kategorií osobních údajů, jimiž jsou údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení.“[96]

Je třeba zmínit změnu, jež nastává s nařízením v kategorii citlivé údaje, kam nově patří genetické údaje, biometrické údaje a též osobní údaje dětí. „Genetickými údaji jsou osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby.“[97] Pod pojmem genetické údaje jsou myšleny údaje, jež se týkají zděděných nebo získaných genetických znaků konkrétní fyzické osoby vyplývající z analýzy biologického vzorku či jiného prvku dotčené fyzické osoby, jež umožňuje získat relevantní informace. „Biometrickými údaji jsou osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.“[98] Údaje vyplývající z konkrétního technického zpracování, jež se týkají fyzických či fyziologických znaků a umožňují tak jedinečnou identifikaci jsou biometrické údaje. Typické pro tyto údaje je například otisk prstu, fotografie obličeje, ale v neposlední řadě i podpis.[99] Dále GDPR

[95] 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/E

[96] GDPR – Obecné nařízení o ochraně osobních údajů: Co je GDPR a jak bude aplikováno v Česku [online] Škorničková, E., [cit. 25.3.2017] dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

[97] 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/E

[98] 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/E

[99] GDPR – Obecné nařízení o ochraně osobních údajů: Co je GDPR a jak bude aplikováno v Česku [online] Škorničková, E., [cit. 25.3.2017] dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

za osobní údaje považuje informace o zdravotním stavu, do nichž by měly být zahrnuty nejen informace o fyzickém stavu osoby, které se údaje týkají, ale i o duševním stavu. Vyloučeny z působnosti GDPR jsou veškeré anonymizované údaje, údaje osob zemřelých, dále shromážděné údaje pro osobní potřebu, tudíž nebudou tyto údaje použity pro obchodní ani jinou sdílenou činnost. „Zvažuje tedy problém ochrany údajů i uvnitř společnosti, zaměstnanců a lidských zdrojů (HR) jakož i směrem ven orientovanou problematiku na zákazníka a uživatele.“[100]

U tohoto nového nařízení je vzhledem k moderním trendům neustálého technologického rozvoje a globalizace kladeno mezi hlavní cíle poskytnout podnikatelským subjektům výhody, jež nabízí jednotný digitální trh, současně nastolit důvěru v rozvoj digitální ekonomiky ve vnitřním trhu a to převážně na základě jednotné roviny ochrany fyzických osob. Doposud platná směrnice 95/46/ES stanovovala povinnost ohlašovat dozorovým orgánům zpracovávání osobních údajů, což představuje zátěž pro společnosti, nicméně zlepšení ochrany osobních údajů se tím neprokázalo. Nařízením GDPR bude tato povinnost zrušena a nahrazena jinými postupy a mechanismy. Též bude zaveden nový princip tzv. zodpovědnosti správců a zpracovatelů, který bez ohledu na velikost společnosti a počet zaměstnanců nařizuje zavést technická, organizační i procesní opatření v souladu s principy GDPR.[101] Opatření se budou vztahovat k oblastem:

- implementace záměrné a nezbytné ochrany dat
- vypracování posouzení vlivu na ochranu osobních údajů, v angličtině DPIA neboli Data Protection Impact Assessment
- jmenování pověřence pro ochranu osobních údajů neboli DPO (Data Protection Officer)
- zavedení tzv. pseudonymizace osobních údajů
- vedení záznamů o činnostech zpracování
- konzultace s dozorovým orgánem před samotným zpracováním osobních údajů[102]

DPIA je novinkou v ochraně osobních údajů, jedná se v podstatě o posouzení dopadu na ochranu dat, kdy společnosti při provádění systematických a rozsáhlých vyhodnocování

[100] Lambert, P., The Data Protection Officer: Proffesion, Rules and Role. 2017 by Taylor and Francis Group, LLC, [volný překlad z AJ]

[101] Právní prostor: První výkladová pravidla k GDPR, [online] 30.1.2017, Nešpůrek R., [cit. 25.3.2017] Dostupné z: http://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/h-prvni-vykladova-pravidla-k-gdpr

[102] GDPR – Obecné nařízení o ochraně osobních údajů: Co je GDPR a jak bude aplikováno v Česku [online] Škorničková, E., [cit. 25.3.2017] dostupné z: https://www.gdpr.cz/gdpr/povinnosti/

údajů založené na automatizovaném zpracování, které je často tvořeno za účelem další nabídky, budou muset toto posouzení vlivu vypracovat. Významnou skupinou, jež tato administrativní povinnost zasáhne, jsou hlavně telekomunikační služby. Nicméně obdobné povinnosti se nevyhnou ani instituce jako jsou zdravotní pojišťovny, nemocnice i bezpečnostní agentury. Pro doložení souladu s GDPR je správce povinen přijmout interní koncepce, upravit procesy včetně zavedení náležitých opatření, pro dodržení ochrany osobních údajů. Hlavní zásadou by měla být minimalizace, v následné rychlé pseudonymizaci a transparentnosti s ohledem na jejich účel zpracování včetně přístupu subjektů k jejich údajům.[103] „Pseudonymizací je 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.“[104] Pseudonymizace je v podstatě zpracování osobních údajů, tak aby již nemohly být přiřazeny k žádnému konkrétnímu subjektu bez použití dodatečných dat. Tyto dodatečná data mají být uchovávána odděleně a chráněna. Další princip, jímž je vedení záznamů o činnostech zpracování správcem i zpracovatelem, je pro monitorování zpracovávaných operací, které budou na vyžádání předkládány dozorovému úřadu. „Monitorování souladu s tímto nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů.“[105] Záznamy musí obsahovat tyto informace jako je jméno a kontaktní údaje správce a zpracovatele, účel zpracování údajů, popis kategorií, informace o předáváním osobních údajů mezinárodně, lhůty pro výmaz kategorií a popis opatření technických i organizačních. „Řádné fungování vnitřního trhu vyžaduje, aby volný pohyb osobních údajů v Unii nebyl z důvodů souvisejících s ochranou fyzických osob

[103] Právní prostor: K některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů (GDPR), [online] 25.2.2016, Burian, D., [cit. 25.3.2017] dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/k-nekterym-povinnostem-ktere-pro-spravce-prinasi-gdpr

[104] 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/E

[105] 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/E

v souvislosti se zpracováním osobních údajů omezen ani zakázán. Aby byla zohledněna specifická situace mikropodniků a malých a středních podniků, obsahuje toto nařízení odchylku pro organizace s méně než 250 zaměstnanci týkající se uchovávání údajů. Kromě toho jsou orgány a instituce Unie, členské státy a jejich dozorové úřady podporovány v tom, aby specifické potřeby mikropodniků a malých a středních podniků zohledňovaly při uplatňování tohoto nařízení.“[106] Pro společnosti s méně než 250 zaměstnanci a v případě, že zpracování osobních dat není hlavní náplní společnosti, nehrozí u nich riziko ohrožení práva a svobody a nezpracovávají citlivé údaje subjektů, je jim v tomto případě udělena výjimka a nemusí vést záznamy o činnostech zpracování. „Důležitým pilířem prokazování souladu s GDPR je jmenování tzv. pověřence pro ochranu osobních údajů neboli DPO (Data Protection Officer).“[107] Primárně je hlavním úkolem tohoto pověřence monitorování shody mezi zpracování osobních údajů s nařízením EU včetně vnitřních auditů, školeních a kontroly globální agendy ochrany dat uvnitř společnosti. „Správce a zpracovatel zajistí, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů.“[108] Pověřenec nemusí být osoba znalá právních předpisů, ale tato osoba s odbornými znalostmi právních předpisů by mu měla být nápomocna.

„Změny, jež GDPR přináší v oblasti sankcí za porušení regulace ochrany osobních údajů, jsou zásadní. V první řadě dojde k posilnění pravomocí a mezinárodní spolupráce mezi vnitrostátními dozorovými orgány“[109] Sankce se oproti nynějším limitům podstatně zvýší a zpřísní jejích uplatňování. Dozorové orgány mohou za nejzávaznější správní delikty uložit pokutu až do výšky 20 milionů EUR, popřípadě do 4 % z celkového ročního obratu podnikatele, popřípadě za předchozí účetní rok, podle toho, která částka bude vyšší.[110] Tímto nařízením

---

106 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/E

107 GDPR – Obecné nařízení o ochraně osobních údajů: Co je GDPR a jak bude aplikováno v Česku [online] Škorničková, E., [cit. 25.3.2017] dostupné z: https://www.gdpr.cz/gdpr/dpo/

108 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/E

109 GDPR – Časť 1: Najzásadnejšie zmeny, ktoré prinesie európska reforma ochrany osobných údajov [online] 5.2.2017 [cit. 27.11.2017] Dostupné z: http://www.steiniger.org/sk/clanky/gdpr-cast-1-najzasadnejsie-zmeny-ktore-prinesie-europska-reforma-ochrany-osobnych-udajov

110 ITGP Privacy Team, The EU General Data Protection Regulation (GDPR): A Practical Guide, Second edition published in the United Kingdom, str. 290 [volný překlad z AJ]

dosáhne EU i u největších společností s technologickým zaměřením, kteří nejvíce těží ze správy osobních údajů.

3.4 Shrnutí

Chystané právní úpravy nařízením Evropského parlamentu a Rady (EU) 2016/679 (3.3.2.) 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 (3.1.1.), která vstoupí v platnost dnem 25. května 2018 ve všech členských státech Evropské unie, by měly usnadnit nejen kontrolu subjektům, jejichž osobní údaje jsou zpracovávány, ale i hájit a chránit jejich práva ve všech státech EU. Jedná se o revoluční legislativu pod zkratkou GDPR (General Data Protection Regulation), která má za úkol výrazně zvýšit ochranu osobních dat a informací, neboť současná legislativa již nedostačuje. Díky neustálému rozvoji technologie je současná legislativa již zastaralá. Při jejím vývoji nebyly ještě sociální sítě, ani cloudová uložiště či chytré telefony. Tak s největší pravděpodobností i nové nařízení v době vstoupení v platnost, již bude díky nezadržitelnému technologickému rozvoji pravděpodobně opět zastarávat. Toto nařízení se dotkne všech odvětví i v podstatě všech občanů členských států. Krok, jež podnikla Evropská unie na ochranu osobních údajů fyzických osob, je další postup ke zlepšení ochrany osobních údajů všech osob.

V současnosti je nezbytné se i nadále řídit platnou právní úpravou, jež je určována zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (3.1.2.). Tato platná právní úprava v souladu s legislativou Evropské unie, která je zastoupená pro tento případ Směrnicí Evropského parlamentu a Rady 95/46/ES (3.1.1.) určuje legislativně, jak zpracovávat osobní údaje v souladu s jejich ochranou. Určuje správci (3.2.4.) a správcem určenému zpracovateli jejich povinnosti, jak s těmito údaji pracovat a následně naložit, aby tím nebyla poškozena ochrana subjektů. Správce musí mít stanoveno, za jakým účelem data shromažďuje a po jakou dobu budou tyto data u správce drženy, kdy kontrolou podléhá Úřadu pro ochranu osobních údajů. Z jeho strany může být i sankcionován. K mobilním operátorům se vztahuje i zákon č. 127/2005 Sb., o elektronických komunikacích (3.3.1.), a o změně některých souvisejících zákonů. Nejdůležitější podmínka, jež musí být uplatněna vždy, když je pracováno s osobními údaji, je souhlas subjektu se zpracováním jeho dat. Úzce spjatý s elektronickými komunikacemi, a tudíž i s mobilním operátorem je i zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb.

a zákona č. 205/2017 Sb., jímž jsou upravovány práva i povinnosti poskytovatelů elektronických komunikací. Zároveň upravuje v součinnosti s předpisy Evropské unie zajišťování bezpečnosti v kybernetickém prostoru.[111] Kybernetický prostor je stěžejní prostředí pro vznik a zpracování informací včetně výměny v sítích elektronických komunikací. Tento virtuální prostor nezná hranic a z tohoto důvodu musí neustále čelit různým kybernetickým útokům. Vzhledem k neustálému rozvoji informačních technologií je nejdůležitějším orgánem v zajišťování kybernetické bezpečnosti Národní bezpečnostní úřad, jež úzce spolupracuje s národním a vládním dohledovým pracovištěm CERT.[112]

Současně bylo nezbytné komplexně vyložit, co jsou osobní údaje (3.2.1.), identifikační údaje (3.2.2.) a hlavně neustále řešené citlivé údaje (3.2.3.). U těchto údajů bývá někdy složité správné rozřazení. Lidé často zaměňuji citlivé údaje za osobní údaje. Dochází k neschopnosti své osobní údaje správně identifikovat a následně s nimi i správně nakládat. [113]

[111] Viz zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb.

[112] Viz zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb.

[113] Viz Zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016

4 Vlastní práce

4.1 Mobilní operátor T-Mobile Czech Republic a.s.

4.1.1 Krátké představení mobilního operátora

Součástí mezinárodní telekomunikační skupiny Deutsche Telekom je kromě Německa, USA, Spojeného království (GB), Nizozemska, Rakouska, Slovenska, Chorvatska, Polska, Maďarska, Makedomie, Černé Hory i Česká republika a to pod obchodní značkou T-Mobile Czech Republic akciová společnost vlastnící stejnojmennou síť GSM , kterou začala provozovat v roce 1996 firma Radiomobil a.s. tehdy ještě pod značkou Paegas.[114] „T-Mobile převzal spolu s EuroTelem dne 25. března 1996 pověření k provozování sítě GSM a krátce nato vytvořil akciovou společnost RadioMobil a.s., jež se také stala provozovatelem sítě Paegas.“[115]

Základním posláním společnosti T-Mobile Czech Republic bylo a je podle stanoveného rozsahu obchodních aktivit vytvářet a provozovat veřejnou mobilní telekomunikační síť ve standardu GSM 900 a 1800 MHz, v souladu s licencemi pro provoz veřejné mobilní telekomunikační sítě vydanými Ministerstvem průmyslu a obchodu a Českého telekomunikační úřadu, a dále poskytovat mobilní telekomunikační služby k nim příslušející.

Pro představu o společnosti T-Mobiel CzechRepublic a.s. a o tom jaké množství dat svých zákazníků zpravuje, je nezbytné zmínit alespoň několik posledních let jejího vývoje. Ačkoliv negativní trendy na trhu, jako jsou vysoká míra nasycení mobilního trhu, velmi silná konkurence a regulační opatření ze strany Evropské Unie, vzrůstaly, byl rok 2010 pro T-Mobile především ve znamení integrace, a to jak integrace nových služeb, tak i organizačních složek. Opakovaně se podařilo mobilnímu operátorovi potvrdit svou přední pozici na trhu. Průměrná měsíční útrata za zákazníka v telekomunikačních službách dosáhla 417 Kč. Společnost T-Mobile CZ absolvovala externí prověrku se zaměřením na opatření a procesy zamezující korupci. Meziroční srovnání k 31.12.2010 ukázalo,

[114] T-Mobile Czech Republic a.s., Historie mobilních komunikací, 10. Výročí založení společnosti, Praha 2006, ZRDISC 4424

[115] iDnes.cz: Mobilní komunikace v České republice zúčtování před ComNetem [online]. 8.6.1997, [cit.24.10.2016] Dostupné z: http://mobil.idnes.cz/mobilni-komunikace-v-ceske-republice-zuctovani-pred-comnetem-pt8-/

že finální počet aktivních zákazníků k tomuto datu činil 5,5 milionů, z čehož bezmála 2,8 milionů bylo tarifních uživatelů.[116] Tento rok se vyznačoval velmi intenzivním budováním sítě 3G[117]. „Po letech letargie se naši operátoři probrali a začali konečně rozumným tempem budovat 3G sítě. T-Mobile ale šel ještě o krok dál a rovnou začal aplikovat tu nejmodernější technologii na daném poli. A to jako jeden z prvních mobilních operátorů na světě.“[118]

V roce 2011 oslavil T-Mobile Czech Republic a.s. patnáctileté výročí působení na českém trhu. Též byla uzavřena operátorem smlouva o sdílení 3G sítě se společností Telefónica, kdy dohoda se týkala ještě nepokrytých oblastí. 2011 je rokem ve znamení prudkého vzestupu a rozvoje datových služeb. Společnost investovala hlavně do vysokorychlostní sítě. I to přispělo ke vzrůstu o 34 % v objemu přenesených mobilních dat uživateli. I tak však operátor zaznamenal výrazné snížení průměrné útraty za zákazníka, i přesto že se spotřeba telekomunikačních služeb poměrně obecně u všech operátorů zvýšila. Operátor zachoval opět trend růstu počtu zákazníků, dosáhl počtu 5,4 milionů zákazníků. I nadále docházelo k růstu zákazníků využívajících některý z paušálních tarifních programů. Jednalo se o 53 % ze zákaznické základny, což byl počet 2,9 milionů aktivních uživatelů.[119]

Rok 2012 u T-Mobile by bylo vhodné nazvat rokem „rychlých dat“. Stále bylo prioritou operátora rozšiřovat a zrychlovat svou 3G síť, jež je brána z hlediska nezávislého dlouhodobého hodnocení jako nejrychlejší. Operátor dále otestoval a pilotně nasadil LTE[120] technologii na níž byl původně zaměřen již před 3G sítí, a zrychlil i pevné připojení. I oblast ICT služeb pokračovala v rozvoji. Nárůst zákazníků již nemá tendenci rychlého vzestupu, zvýšil se o 117 tisíc tj. 2,2 % na téměř 5,5 milionů zákazníků z nichž 2,9 milionů využívá některý z tarifních programů, což je 56 % tarifních zákazníků. Operátor si i nadále drží

---

[116] T-Mobile Czech Republic a.s.: Výroční zpráva 2010, dostupná: http://www.t-mobile.cz/dcpublic/Annual_report_2010_CZ.pdf

[117] Síť 3G neboli síť 3. Generace umožňuje vysokorychlostní komunikační služby a asymetrické datové přenosy, podporuje internet a IP přenosy, videokonference, dále umožňuje vyšší kapacitu sítě, podporuje simultánní datové a hlasové přenosy s dostupností pro 86 % populace ČR.

[118] iDnes.cz: Ceny redakce Mobil.cz aneb to nejlepší z mobilního roku 2010 [online] Vokáč, Luděk 7.2.2011 [cit. 31.10.2016] Dostupné z: http://mobil.idnes.cz/

[119] T-Mobile Czech Republic a.s.: Výroční zpráva 2011, dostupná: http://www.t-mobile.cz/dcpublic/Annual_report_2011_CZ.pdf

[120] LTE technologie jehož zkratka pochází z anglického názvu 3GPP Long Term Evolution, což je technologie určená hlavně pro vysokorychlostní internet v mobilních sítích, která formálně spadá do standardu 3G, přičemž její následovník LTE Advanced bude již plnohodnotné 4G řešení.

prvenství na trhu, i když opět došlo k výraznému poklesu průměrné útraty za zákazníka na 362 Kč. Navzdory tomu spotřeba telekomunikačních služeb stále rostla.[121]

Následující rok historie společnosti proběhl ve znamení zásadních změn, na trhu se objevily desítky virtuálních operátorů a následkem toho došlo k výraznému snížení cen v mobilním sektoru. Následně se odehrála aukce vysokorychlostních kmitočtů i akvizice, od které se očekávalo, že s velkou pravděpodobností změní rozložení sil. Opět se opakovala situace nárůstu zákazníků ve všech směrech na 5,8 milionů, naopak se opakoval pokles průměrné útraty na zákazníka.[122] „„Rok 2013 vnímám jako nelehký, ale úspěšný. Udrželi jsme vedoucí pozici v mobilním segmentu a v aukci získali frekvence, které nám v budoucnosti umožní další rozvoj naší nejrychlejší sítě," říká Milan Vašina, generální ředitel T-Mobile, a dodává: „Loňský rok nám přinesl také velkou příležitost v B2B segmentu: akvizice T-Systems Czech Republic významně posílí naše kompetence v této oblasti. V uspokojivých finančních výsledcích se mimo jiné odrazila naše neustálá snaha o maximální interní efektivitu.““[123] Komerčně byla spuštěna první část LTE sítě (v Praze a Mladé Boleslavi). „Deutsche Telekom získává skupinu GTS Central Europe." [124] Dále dochází ke sjednocení aktivity T-Mobile a T-Systems na českém trhu. Důležitá událost z oblasti sportu nastala, když se T-Mobile stal oficiálním partnerem českého olympijského týmu.[125]

Opravdu úspěšný rok pro společnost T-Mobile byl rok 2014. Byla dokončena fúze s GTS Czech a T-Systems, čímž byla završena cesta plně integrovaného operátora a mimo jiné se významně posílila pozice operátora v B2B segmentu. Z hlediska provozního i finančního společnost dosáhla svých cílů. Došlo k zjednodušení akcionářské struktury, kdy Deutsche Telekom se stal jediným akcionářem, neboť získal zbývající menšinový podíl. Co do počtu zákazníku byla konečně překročena hranice 6 milionů aktivních zákazníků, ale průměrná měsíční útrata na zákazníka stále klesala již na 263 Kč. I nadále operátor investoval do budování vysokorychlostních sítí 3G a LTE.[126] „Operátoři Telefónica

---

[121] T-Mobile Czech Republic a.s.: Výroční zpráva 2012, http://www.t-mobile.cz/dcpublic/Annual_report_2012_CZ.pdf

[122] Echo – interní magazín společnosti T-Mobile, registrace: MK ČR E 10161

[123] T-Mobile Tiskové centrum: T-Mobile: 2013 – Rok plný změn, [online] 6.3.2014 [cit. 31.10.2016] Dostupné z: http://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/t-mobile-2013-rok-plny-zmen.html

[124] Echo – interní magazín společnosti T-Mobile, registrace: MK ČR E 10161 str. 7

[125] Echo – interní magazín společnosti T-Mobile, registrace: MK ČR E 10161

[126] T-Mobile Tiskové centrum: 2014: T-Mobile Czech Republic ohlašuje úspěšný rok [online] 26.2.2015 [cit.31.10.216] Dostupné z: http://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/2014-t-mobile-czech-republic-oznamuje-uspesny-rok.html

a T-Mobile plánují sítí LTE ještě letos společně pokrýt většinu území Česka. Proti tomuto záměru již dříve protestoval další konkurent Vodafone.“[127]

I rok 2015 setrval pro společnost T-Mobile jako úspěšný a inovativní, kdy se operátor rozhodl plně soustředit na monetizaci mobilních dat a rozvoj možností v segmentu firemních zákazníků, jež společnost získala akvizicemi GTS a T-Systems. Pokračovalo zaměření na rychlé rozšíření LTE sítě, kdy na konci roku bylo dosaženo 82 % pokrytí populace a 80 % z celého území ČR. Byla uvedena řada inovací jako je Voice over LTE a Voice over Wi-Fi či řešení pro handicapované zákazníky. Společnost i nadále investuje do rozvoje technologii a tím posiluje svou pozici technologického leadera. Prokázalo se, že strategie integrovaného operátora je správná, neboť operátor zaznamenal vzrůst tržeb o 12,5 %. Stále stoupá datová spotřeba, a naopak je zaznamenám opakovaný pokles průměrné měsíční útraty na zákazníka.[128] Akcionáři rozhodly o jmenování současného generálního ředitele pro společnost T-Mobile Czech Republic a.s. i na pozici generálního ředitele Slovak Telekomu, kdy bude obě pozice zastávat současně. Jedná se o klíčový krok, kterým má být posílena pozice Deutsche Telekomu ve střední Evropě.[129]

Tento rok 2016 respektive první polovinu tohoto roku vykazuje společnost stabilní výkonnost a velmi dobré výsledky, jež potvrdily, že strategie tohoto již plně integrovaného operátora jsou správné. Nadále pokračuje zaměření na B2B trh stejně jako v předchozích letech. Operátor rozšířil svou nabídku o řadu dalších služeb a produktů, předně se jedná o nabídku T-Mobile TV, nové Twist a roamingové datové balíčky a mimo jiné virtuální datové centrum. „T-Mobile spustil Wi-Fi volání do komerčního provozu i pro tarifní zákazníky.“[130] Oproti stejnému období v předchozím roce se zvýšila spotřeba mobilních služeb zvláště

[127] iDnes.cz: Ještě letos Telefónica a T-Mobile společně pokryjí většinu Česka LTE [online] ČTK, vse 5.5.2014 [cit. 31.10.2016] Dostupné z: http://mobil.idnes.cz/telefonica-a-o2-sdileji-lte-dcg-/mobilni-operatori.aspx?c=A140505_095129_mobilni-operatori_vse

[128] T-Mobile Tiskové centrum: T-Mobile oznamuje úspěšný a inovativní rok [online] 24.2.2016 [cit.31.10.2016] Dostupné z: http://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/t-mobile-oznamuje-uspesny-a-inovativni-rok.html

[129] T-Mobile Tiskové centrum: Milan Vašina generálním ředitelem skupiny Slovak Telekom [online] 23.12.2015 [cit.31.10.2016] Dostupné z: http://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/milan-vasina-generalnim-reditelem-skupiny-slovak-telekom.html

[130] T-Mobile Tiskové centrum: Wi-Fi volání je dostupné pro všechny tarifní zákazníky [online] 31.3.2016 [cit.2.11.2016] Dostupné z: http://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/wi-fi-volani-je-dostupne-pro-vsechny-tarifni-zakazniky.html

v oblasti dat. Současně byla tvořena nová organizační a personální struktura společnosti pro vytvoření funkční spolupráce mezi T-Mobilem a Slovak Telekomem. Jako první operátor spustila společnost T-Mobile Projekt zaměstnání odsouzených v call centru. Jedná se o pomoc zvýšení zaměstnanosti odsouzených, jež by mělo napomoct vyhnout se dalšímu páchání trestné činnosti a lepší integraci do společnosti. Call centrum je vybudované přímo ve vězeňskému nápravném zařízení ve Věznici Vinařice. Tato inovace je podporována i Evropským sociálním fondem. Tento rok uběhlo již 20 let, co T-Mobile vstoupil na český trh a neustále upevňuje svou pozici.[131]

4.1.2 Závěr představení mobilního operátora

Mobilní operátor T-Mobile je od svého vstupu na český trh neustále se rozvíjející společnost momentálně spravující data více jak 6,02 mil zákazníků. Tato skutečnost nutí operátora neustále zdokonalovat své procesy a investovat do mnohaletého vývoje pro ochranu dat a informací. Ochrana osobních údajů je klíčovým zájmem napříč celou skupinou Deutsche Telekom a tím se stává i jedním z cílů politiky této skupiny, kdy je definována politika pro adekvátní bezpečnostní standart ochrany veškerých dat a informací včetně osobních údajů pro celou skupinu Deutsche telekom. Dlouhodobě též T-Mobile spolupracuje s týmem hackerů pro odstranění veškerých nedostatku, kdy by bylo možné nabourat síť a poškodit tím zákazníky společnosti. Současně neustupuje v procesu proti selhání lidského faktoru v podobě svých zaměstnanců.

4.2 Ekonomická část – Mobilní operátor součástí koncernu

Společnost T-Mobile Czech Republic a.s. je součástí koncernu mezinárodní telekomunikační skupiny Deutsche Telekom. „Jedna nebo více osob podrobených jednotnému řízení (dále jen "řízená osoba") jinou osobou nebo osobami (dále jen "řídící osoba") tvoří s řídící osobou koncern.“[132] Jedná se tedy o holding, což je v podstatě sdružení korporací. „Jednotným řízením je vliv řídící osoby na činnost řízené osoby sledující za účelem dlouhodobého prosazování koncernových zájmů v rámci jednotné politiky koncernu koordinaci a koncepční řízení alespoň jedné z významných složek nebo činností

[131] Echo – interní magazín společnosti T-Mobile, registrace: MK ČR E 10161
[132] § 79 zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších přepisů

v rámci podnikání koncernu.“[133] Charakteristikou tohoto holdingu je, že jedna společnost holdingová neboli mateřská společnost na základě kapitálového vlastnictví v tomto případě nadpoloviční většiny akcií či popřípadě na základě jiných skutečností ovládá a usměrňuje jednu i více společností. Všem společnostem, jež jsou součástí takového koncernu zůstává právní subjektivita. Tyto holdingové společnosti mají nejčastěji právní formu akciové společnosti. V České republice je koncern neboli holding upraven v § 71–91 zákona č. 90/2012 Sb., o obchodních korporacích.

V případě společnosti T-Mobile se jedná o akciovou společnost, což je nejrozšířenější právní forma podnikání kapitálové společnosti a je převážně regulována evropským právem. Kapitál společnosti je rozvržen do určitého počtu akcií. „Bonn, Praha, 10. února 2014 – Deutsche Telekom oznámil odkoupení zbývajících 39, 23 % akcií T-Mobile Czech Republic (T-Mobile CZ) za cenu 0,8 miliardy EUR. Vlastníkem tohoto podílu je konsorcium investorů.“[134] Akcie je cenný papír, ke kterému se pojí práva akcionáře jako společníka společnosti na řízení, zisku i v případě zrušení společnosti na možném likvidačním zůstatku. Akcionáři neručí za závazky společnosti. Tyto cenné papíry mají jmenovitou neboli nominální hodnotu, která je uvedena na akcii a také kurzovní hodnotu, což je tržní hodnota akcie pro nákup a prodej. V současné době je 100 % vlastníkem akcií české společnosti T-Mobile německá společnost Deutsche Telekom, tím je umožněna zjednodušená kapitálová i správní kontrola. Tato transakce poskytla nemalé výhody v podobě úspora na vyplácení ročních dividend minoritním vlastníkům akcií a zároveň zvýšení čistého zisku společnosti. Tímto krokem byla dovršena plná konsolidace k Deutsche Teekomu a tato transakce nebude mít tedy žádný dopad na příjmy. [135]

Do orgánů akciové společnosti patří valná hromada, představenstvo a dozorčí rada. Nejvyšší orgán akciové společnosti je valná hromada neboli shromáždění všech akcionářů. Při přítomnosti akcionářů, kdy akcie přesahují jmenovitou hodnotu 30 % ze základního kapitálu, je valná hromada usnesení schopná. Rozhodování valné hromady je na základě většiny

---

[133] § 79 zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších přepisů

[134] T-Mobile Tiskové centrum: DEUTSCHE TELEKOM KUPUJE ZBÝVAJÍCÍ AKCIE T-MOBILE CZECH REPUBLIC [online] 10.2.2014 [cit. 20.3.2017] dostupné z: https://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/deutsche-telekom-kupuje-zbyvajici-akcie-t-mobile-czech-republic.html

[135] T-Mobile Tiskové centrum: DEUTSCHE TELEKOM KUPUJE ZBÝVAJÍCÍ AKCIE T-MOBILE CZECH REPUBLIC [online] 10.2.2014 [cit. 20.3.2017] dostupné z: https://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/deutsche-telekom-kupuje-zbyvajici-akcie-t-mobile-czech-republic.html

hlasů, ale hlas akcionáře řídí jmenovitá hodnota akcie. Mezi hlavní činnosti valné hromady patří rozhodnutí o zvýšení, anebo případné snížení základního kapitálu, změna stanov, volba členů představenstva, ale stejně tak i jejich odvolání, volba, ale zároveň i odvolání členů dozorčí rady, schválení roční závěrky, zároveň schvaluje rozdělení zisku a má pravomoc na rozhodnutí o zrušení společnosti.[136]

Statutárním orgánem akciové společnosti je představenstvo, které má nejméně tři členy, jež volí svého předsedu. Představenstvo rozhoduje o záležitostech společnosti, pokud tato kompetence není vyhrazena valné hromadě. Představenstvo má povinnost zastupovat společnost vůči třetím i před soudem. Mezi další povinnosti představenstva patří vytváření a řízení práce společnosti, včetně zabezpečení vedení účetnictví a následně předkládá roční účetní závěrku valné hromadě ke schválení s návrhem přerozdělení zisku.[137]

Nejvyšším kontrolním úřadem akciové společnosti, jež dohlíží na činnost představenstva, je dozorčí rada. Musí se skládat minimálně ze tří členů, ale ty mohou být zároveň členy představenstva. Členové dozorčí rady mají pravomoc nahlížet do všech dokladů, které se týkají společnosti včetně kontroly účetnictví, zároveň mezi jejich povinnost patří přezkoumání správnosti roční závěrky i návrhu rozdělení zisku. Zpráva valné hromadě předkládá dozorčí rada. [138]

4.3 Organizační struktura společnosti se zaměřením na bezpečnost

Organizační struktura společnosti T-Mobile Czech Republic a.s. je poměrně spletitá a v podstatě by bylo možné uvést, že na ochraně osobních údajů a informací zákazníků se podílí celá společnost. Ovšem pro přesný obrázek o struktuře, jak tato společnost pracuje, je důležité vytyčit konkrétní divize, jež se touto problematikou zabývají.

1. CEO Division – sekce generálního ředitele
    - 2. Legal and Corporate Affairs Division – Divize právních a firemních záležitostí

[136] Hes, A., Regnerová, M., Hrubá, D., Obchodní nauka. Praha: PEF ČZU, 2007 (dotisk). ISBN 80-213-1155-X
[137] Hes, A., Regnerová, M., Hrubá, D., Obchodní nauka. Praha: PEF ČZU, 2007 (dotisk). ISBN 80-213-1155-X
[138] Hes, A., Regnerová, M., Hrubá, D., Obchodní nauka. Praha: PEF ČZU, 2007 (dotisk). ISBN 80-213-1155-X

Tuto divizi tvoří veškerá právní oddělení jako je B2B, Corporate, B2C, FIN, HR. Jejich úkolem je zajištění právní podpory komplexně včetně administrativy.

- 2.1. Legal Affairs Unit CZ - Oddělení právních záležitostí – Tato divize má na starosti komunikaci s ČTÚ a Národním bezpečnostním úřadem.
  Přímo na tuto sekci navazuje oddělení DATA PRIVACY TEAM – Tým ochrany dat – tento tým zajišťuje veškerou ochranu osobních údajů zákazníků
- 2.2. Corporate Security Unit CZ – Firemní bezpečnostní jednotka – tato divize nevytváří individuální nastavení, ale vytváří strategii a politiku společnosti jako celku. Zajišťuje legislativu, hodnocení požadavků z hlediska kritičnosti, ochranu informací. Patří se oblast identity managementu, což jsou procesy a nástroje na podporu přístupů do systému. Bezpečností se zabývá celý útvar, tzn několik menších týmů jako je sekce
- Oddělení bezpečnosti dat a informací,
- Tým ochrany zpracování dat a služeb,
- Tým vnitřního vyšetřování služeb – zde vyšetřovány všechny incidenty (podvody – zákazník, zaměstnanec),
- Tým fyzické bezpečnosti – tento tým chrání pracoviště po fyzické stránce

Oddělení, které řeší ochranu dat a informací z technologického hlediska je

- Regional Security Services Department – Oddělení regionální bezpečností služby, stará se o bezpečné fungování systému.
  regionální bezpečnostní služby oddělení. Patří pod Technology Security Unit – Jednotka bezpečnostní technologie, kdy pokud se podíváme dle hierarchie výše je tato jednotka podřízena Divizi technologie a IT – Technology and IT Division
- Vytváří závazná pravidla, nastavení, vykonává požadavky i individuální požadavky. Řeší obvyklé standardy, a to komu a kam se data předávají. Mezi kompetence tohoto oddělení patří testování, penetrační testy, kontrola úrovně bezpečnosti i v provozu, pravidelná aktualizace z důvodu posílení bezpečnosti, provádí každý týden scanování na zranitelnost internetu, detekce zranitelnosti v rámci bezpečnosti,

dlouhodobá spolupráce s týmem hackerů za odměnu, pravidelný report stavu = běžný stav

-

4.4 Ochrana osobních informací a dat procesně

4.4.1 Ochrana osobních údajů v praxi u T-Mobile

V souladu se zákonem 101/2000 Sb. O ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších přepisů je nezbytné pro mobilního operátora T-Mobile se těmito nařízeními řídit a systematicky zpracovávat údaje, ať už se jedná o automatizované přijetí údajů či dalšími prostředky. Na nahodilé shromažďování osobních údajů při podmínce, že nejsou a nebudou dále zpracovány, se toto pravidlo nevztahuje.

Oprávněný útvar společnosti pro zpracovávání osobních údajů zákazníků je například Úsek prodeje a služeb zákazníkům, Finanční úsek, Úsek marketingu. A zároveň s těmito údaji mohou pracovat pouze pověření zaměstnanci, jež mají k práci s těmito údaji oprávnění v souvislosti s výkonem práce uvedeným v pracovní smlouvě jako stanovení popisu práce. Mezi hlavní způsoby zpracování osobních dat u mobilního operátora patří shromažďování osobních údajů, uchování osobních údajů, blokování osobních údajů a následná likvidace osobních údajů.

Cílem shromažďování osobních údajů operátorem je při systematickém postupu získání těchto údajů uložením na nosič informací, kde dochází k okamžitému případně pozdějšímu zpracování. Při procesu uchování osobních údajů dochází k udržení těchto údajů v podobě, při které je možné tyto údaje dále zpracovávat. Blokování jako způsob zpracování, ponechává údaje ve stavu, kdy po určitou dobu nelze k údaji přistoupit a ani jinak zpracovat. Likvidací operátor zajišťuje trvalou likvidaci, jako je fyzické zničení nosiče, popřípadě vymazání či trvalé vyloučení z dalšího zpracování.

Společnost jakožto správce osobních údajů podléhá dle zákona Úřadu pro ochranu osobních údajů a je povinna oznámit úřadu zpracování osobních údajů. Společnost zpracovává osobní údaje u těchto subjektů: zákazník stávající a bývalý, potencionální zákazník, zákazník předplacených služeb TWIST. Stanoveným účelem zpracování osobních údajů u mobilního operátora je hlavně:

- plnění uzavřené smlouvy a ochrany svých práv
- jednání o smluvním vztahu mezi operátorem a zákazníkem
- plnění povinností, které uvádí zvláštní předpisy

- obchodní a marketingový účel
- pro ověření zletilosti, identity a zhodnocení platební morálky zvláště u potencionálního zákazníka
- dále pro účel zveřejnění kontaktních údajů zákazníka ve službě T-Mobile Assistent pro informační účely veřejného telefonního seznamu

Mezi nadbytečné osobní údaje mobilní operátor bere údaje jako je rodné příjmení, stav, místo narození, fotografie (tento údaj spadá do citlivých údajů), pohlaví i národnost a mnoho dalších údajů.

Mezi primární zájmy mobilního operátora patří ochrana osobních údajů zákazníků, proto neustále investuje do rozvoje technologie. Pro zjednodušení procesu a snížení přístupu k údajům zákazníků vznikla skupina nástrojů pod názvem NGCRM – New Generation Customer Relationship což je skupina nástrojů a procesů pro správu zákazníka, jeho dat a objednávek. Vytvoření programu CRM zjednodušuje proces nejen pro zákazníky, ale i pro interní zaměstnance, jež jsou v přímém kontaktu se zákazníkem. Částečně automatizované CRM funguje v podstatě jako přímé uložiště údajů karty zákazníka, které umožňuje nejen flexibilnější reakci na jeho požadavky, ale i větší ochranu v omezenosti přístupu zaměstnanců a jeho monitoring. Tito zaměstnanci jsou mobilním operátorem pověřeni ke zpracování dat v souvislosti s výkonem práce sjednané pracovní smlouvou. Jejich povinností je nejen dodržovat pravidla jako je neoprávněný přístup k informačním systémům a jeho zamezení neoprávněným osobám, nepořizovat kopie nosičů těchto dat, zachování mlčenlivosti (což trvá i po skončení pracovního poměru), ale zároveň podléhají i kontrole, zda je těchto pravidel dodržováno. Tato kontrola spadá do kompetence Útvaru Compliance a firemní bezpečnosti a Útvaru práva, regulace a vnějších vztahů, samozřejmě podléhá kontrole i nadřízeného zaměstnance.

4.4.2 Proces anonymizace osobních údajů zákazníků

Mobilní operátor T-Mobile Czech Republic je povinen, jakmile pomine účel, za jakým byla data zákazníků zpracovávána dle platné právní úpravy zákona č. 101/2000 Sb. o ochraně osobních údajů a zákon 127/2005 Sb., o elektronických komunikacích, tyto data zlikvidovat případně anonymizovat. To samé platí pro operátora v případě, že zákazník požádá sám o likvidaci svých osobních údajů. Z důvodu, že operátor poskytuje služby a prodej zařízení, je nezbytně nutné zpracovávat osobní údaje zákazníka ještě následující

tři měsíce od ukončení smlouvy zvláště z možnosti reklamace a v případě zpracování údajů na zhodnocení platební schopnosti – morálky, tyto údaje by měly být anonymizovány nejpozději do tří let od poslední platby závazku vůči operátorovi. Nicméně v případě, že je se zákazníkem vedeno řízení jako reklamační, vymáhací a jiné, je lhůta automaticky prodloužena až po dobu ukončení tohoto řízení. Pokud by nějakým způsobem byla tato povinnost daná zákonem porušena, pak je Úřad na ochranu osobních údajů oprávněn udělit pokutu, a to až do výše 10 mil. Kč. Při běžném pochybení v praxi většinou úřad uděluje pokutu v rozmezí 100 tisíc až 1 mil Kč. Pravidlem tedy je, že pokud nemá zákazník vůči operátorovi žádný dluh, operátor přistupuje k anonymizaci dat neprodleně po deaktivaci i poslední SIM karty zákazníka.

Pro omezení pochybení se snaží operátor o automatizovanou anonymizaci. To znamená, že pokud není zákazník v žádném právním vztahu s operátorem a došlo například k deaktivaci SIM karty, dochází k automatizované anonymizaci dat. Anonymizují se údaje, které operátor získal pro uzavření smlouvy, a to osobní údaje: titul, křestní jméno a příjmení, adresa bydliště, datum narození, rodné číslo, číslo předložených dokladů a stejně tak údaje osob oprávněných jednat za podnikatele. I nadále platí, že z anonymizace jsou vyloučeny údaje účastníků, které jsou potřebné pro vymáhání pohledávek. Vzhledem k tomu, že tento proces je u operátora automatizovaný, musí proběhnout ve všech dotčených systémech podle podmínek k tomu určených. Tato transakce probíhá v pravidelných intervalech. Podmínky pro proces automatické anonymizace jsou, že neplatí žádná podmínka, která by vyloučila zákazníka z procesu anonymizace a další podmínkou je, že byla u daného zákazníka deaktivována poslední smlouva.

Je důležité zdůraznit za jakých podmínek proces anonymizace nenastává. Tyto podmínky jsou:

- pokud je vůči zákazníkovi evidována jakákoliv pohledávka včetně archivované
- v případě, že vůči zákazníkovi není evidována žádná pohledávka, ale existuje zvýšené riziko, neboť byl u něj dluh vymáhán
- zákazník má pohledávku za operátorem
- dále pokud je u zákazníka vytvořen případ – úmrtí, dědické řízení, konkurz, likvidace, insolvenční řízení, úpadek reorganizace, oddlužení na jakékoliv úrovni pod jeho smlouvou.

V případě zaměstnaneckého poměru, kde se jedná o vazbu zaměstnanec x telefonní číslo x provolaná částka, je anonymizace dat poměrně stejná jako u zákazníka. Dochází k ní po uplynutí tří měsíců, které jsou ponechány pro případ možné reklamace jak ze strany bývalého zaměstnance, tak ze strany bývalého zaměstnavatele v tomto případě operátora. V případě možné pohledávky za zaměstnancem ale i naopak zaměstnancem za zaměstnavatelem, kterou nebylo možné umořit s poslední mzdou zaměstnance, je možné toto řešit až po dobu tří let od skončení pracovního poměru.

U mobilního operátora je používám proces archivace zvláště u procesních dat a finančních transakcí mezi, které patří vyúčtování v podobě faktur zvláště pro daňové účely. Dále tomuto procesu archivace podléhají veškeré služby a produkty mobilního operátora.

4.4.3 Bezpečnost informací a ochrana dat u mobilního operátora

Cílem celé skupiny Deutsche Telekom je náležitý bezpečnostní standard se zaměřením na ochranu veškerých informací a dat s důrazem na osobní údaje. Tato politika společnosti je zvláště důležitá z důvodu, kdy obchodní články shromažďují a zpracovávají informace včetně dat, což přispívá a napomáhá k plnění jejich cílů. Pro mobilního operátora jsou data a informace nejdůležitějším ze základních aktiv společnosti, jež potřebuje přiměřenou ochranu. Všechna přijatá opatření na ochranu informací a dat, jsou primárně zřízena na posuzování rizik, vždy je však vyhodnocována možnost nákladové efektivity. Při veškerém jednání společnosti Deutsche Telekom je vždy prioritou důvěryhodnost společnosti a s tím související bezpečné zacházení s osobními informacemi a údaji, na čemž též závisí úspěch společnosti na trhu. Základem pro úspěch v oblasti ochrany informací a dat je jasné vydefinování odpovědností. Odpovědnosti jsou ve společnosti rozděleny dle čtyř základních skupin: lokální bezpečnostní management, vlastníci business procesů, manažeři a zaměstnanci.

Základním bezpečnostním opatřením u lokálního bezpečnostního managementu je komunikování opatření ochrany, podpora a pomoc, zároveň zvyšování podvědomí o opatření zaměstnanců, manažerů a vlastníků procesů a systémů. Součástí bezpečnostního opatření je i pečlivý výběr a schválení zaměstnanců, jež smí nakládat s informacemi a daty s označením „Utajované“ a „Přísně tajné“. Druhá skupina jsou vlastníci business procesů, jejich odpovědnost spočívá v ochraně informací a dat v rozsahu stanoveného procesu a zároveň za formu a rozsah předávání těchto informací z daného procesu. Zvláště pokud jsou informace předávány přes více procesů, je jejich povinností učinit dohody mezi ostatními

vlastníky pro zajištění přiměřené ochrany informací. Zároveň mají povinnost klasifikace a správného označení v systému včetně odpovědnosti za archivaci. Třetí skupina v odpovědnosti jsou manažeři, jejichž základní povinností je komunikace o bezpečnostních požadavcích v rámci svých organizačních jednotek s důrazem na zajištění těchto požadavků. Manažeři jsou povinni zajistit pravidelné školení zaměstnanců, za něž mají i odpovědnost. Čtvrtá základní skupina odpovědnosti jsou všichni zaměstnanci. Ti nesou základní odpovědnost za dodržení požadavků ochrany, co se jejich sféry vlivu týká s důrazem na dosažení splnění pracovních úkolů. Povinností zaměstnanců je v případě jakékoliv pochybnosti s možným ohrožením ochrany informací se obrátit bez prodlení na svého nadřízeného.

Z důvodu z potřeby chránit určité informace jsou dány cíle ochrany. Mezi tyto hlavní cíle ochrany informací patří důvěryhodnost, dostupnost, integrita a autenticita. Což je vyložitelné, že informace nesmí být snadno a běžně dostupná, pouze na vyžádání oprávněné osoby. Informace též musí být uchována úplná a správná, zároveň však musí být i prokazatelně ověřitelný původce a potažmo i příjemce dané informace či data. Správa informace musí projít fází uložení, uchování, zpracování a následné předání, jež musí odpovídat potřebě ochrany informace. Po skončení životnosti informace dochází opět k archivaci a následnému zničení informace po uplynutí zákonné lhůty.

4.5 Dotazníkové šetření

Dotazníkovým šetřením na téma ochrana osobních dat a informací u mobilního operátora měla být ukázána schopnost respondentů, zda vnímají důležitost ochrany svých osobních údajů, jež poskytují svým mobilním operátorům. Dotazníkové šetření probíhalo v elektronické i papírové podobě v období březen až duben 2017 a odpovědělo na něj 300 respondentů. Návratnost a celková úspěšnost dotazníků činí 71,6 %.

Výsledky dotazníku

1. *Využíváte služeb mobilního operát*ora?

Ze stanovených možností Ano – Ne odpovědělo 100 % respondentů, že využívá služeb mobilního operátora.

2. *Jak dlouho již využíváte služeb mobilního operátora (od počátku včetně jakékoliv změny –* v letech)?

U této otázky měli respondenti zaznamenat užívání služeb mobilního operátora v letech bez zaznamenání změn, tzn. přechod k jinému operátorovi, kdy tato otázka měla prokázat dlouhodobé užívání služeb. Užívání služeb v rozmezí 20–16 let uvedlo 43,77 % respondentů, dále 40,63 % respondentů uvedlo užívání služeb mobilního operátora po dobu 15–10 let a 9 – méně let užívání uvedlo 15,63 respondentů.

3. Doplňte prosím název Vašeho operátora……

V této otázce respondenti museli zaznamenat odpověď vlastními slovy a uvést název mobilního operátora, jehož služby užívají. Tato otázka měla prokázat, zda respondenti preferují spíše tři hlavní stěžejní operátory, anebo volí spíše virtuální operátory. Respondenti tedy odpověděli, že T-Mobile užívá 51,56 % respondentů, Vodafone 23,44 % respondentů, služeb O2 – Telefonica využívá 20,32 %, Mobil.cz využívá 1,56 % a stejně tak Tesco mobil i U:fon uvedlo 1,56 % respondentů.

4. Jaké využíváte nabídky u Vašeho mobilního operátora?

Respondent měl u této otázky na výběr ze dvou odpovědí. Nabídka odpovědí byla, užívání Paušálních služeb – Předplacené SIM karty (dobíjení kreditů). Užívání paušálních služeb uvedlo 85,94 % a naopak užívání předplacených karet využívá 14,06 % respondentů.

5. Na další otázky odpovídají pouze zákazníci paušálních služeb: Dával(a) jste při podpisu smlouvy*, popřípadě telefonické objednávce souhlas se zpracováním Vašich osobních údajů?*

Respondent se mohl rozhodnout mezi odpověďmi Ano – Nevím – Ne. Od této otázky je odpovídajících respondentů 256. Se zpracování osobních údajů potvrdilo souhlas, tedy odpověď zněla Ano 58,62 % respondentů, odpověď nevím uvedlo 31,03% respondentů a ne uvedlo 10,34 % dotazovaných.

6. Pokud byla Vaše odpověď ANO, dali jste operátorovi výslovný souhlas se zpracováním Vašich osobních, identifikačních i citlivých údajů?

U otázky 5. odpovědělo 58,62 % respondentů ano. Respondenti měli na výběr Ano – Ne – Nevím. Odpověď nevím na uvedenou otázku uvedlo 60,87 %, odpověď ano potvrdilo 19,57 % respondentů a stejný počet respondentů uvedlo i odpověď ne.

7. Pokud byla Vaše předchozí odpověď ANO, četl(a) jste podmínky pro zpracování Vašich osobních údajů?

Odpovědí ano potvrdilo otázku u předchozí otázky 19,57 % respondentů. Zde měli respondenti na výběr ze čtyř odpovědí Ano – Ne – Nevím – Nepamatuji se. Odpověď ne zvolilo 42,31 % respondentů, nepamatuji se 34,62 %. Podmínky četlo, a tudíž odpovědělo ano 11,54 % respondentů, ale zároveň stejný počet respondentů tj. 11,54 % uvedlo odpověď nevím.

8. V *případě, že byla Vaše předchozí odpověď ANO, byly tyto údaje od operátora srozumitelné?*

Možnost výběru odpovědí byla Ano – Ne. V předchozí otázce odpovědělo kladně 11,54 % respondentů. Z těchto respondentů potvrdilo srozumitelnost údajů 54,55 % respondentů a pro 45,45 % respondentů jsou tyto údaje nesrozumitelné.

9. Pokud byla Vaše odpověď na otázku č. 7 ANO, týkal se Váš souhlas i citlivých údajů jako je třeba kontrola v registru neplatičů ESOX?

Z odpovídajících 11,54 % ano u otázky č. 7, na tuto otázku odpovědělo nevím 53,33 % respondentů, nepamatuji se, uvedlo 26,67 % respondentů a odpověď ne uvedlo 20 % respondentů. Na výběr bylo opět ze čtyř možností odpovědí, což bylo Ano – Ne – Nevím – Nepamatuji se.

10. Zajímal(a) jste se někdy o to, jak dále operátor nakládá s Vašimi údaji?

Respondenti měli na výběr z odpovědí Ano – Ne – Nikdy jsem o tom nepřemýšlel(a). Na tuto otázku odpovědělo 48,44 % ne, nikdy o to nepřemýšlelo 42,19 % respondentů a pouhých 9,38 % respondentů se nad touto otázkou někdy zamyslelo a jejich odpověď zněla ano.

11. Nabyl(a) jste někdy dojmu, že operátor zneužil Vaše osobní data a informace pro jiné účely?

Respondent u této otázky musel zvolit jednu z nabízených odpovědí. Výběr byl z Ano měl(a) jsem podezření – Nikdy mě to nenapadlo – Nevím. S podezřením na zneužití informací a dat se setkalo 39,06 %, nikdy tato možnost nenapadla 32,81 % respondentů a 28,13 % respondentů odpovědělo nevím.

12. Víte, že můžete písemně požádat operátora o výpis všech dat, které o Vás eviduje a pro jaké konkrétní účely je uchovává?

Zde musel respondent zvolit jednu ze tří odpovědí Ano – Ne – Nezajímá mě to. O této možnosti výpisu od operátora neví 78,13 %, kladnou odpověď potvrdilo informovanost 1 7,19 % a zbylých 4,69 % tato možnost nezajímá.

13. Jste seznámeni s informací o možné likvidaci Vašich dat při rozvázání spotřebitelské smlouvy?

Odpovědět mohl respondent Ano – Ne. V tomto případě dopovědělo ne 84,38 % respondentů a pouhých 15,63 % odpovědělo ano.

14. Pokud jste odpověděl(a) ANO u předchozí otázky č. 13, využil(a) jste někdy tohoto práva?

U této otázky byl výběr ze dvou odpovědí Ano – Ne, kdy u předchozí otázky odpovědělo 15,63 % respondentů ano. Na otázku o možnosti využití práva odpovědělo jednoznačně 100 % ne.

15. Máte důvěru ve svého operátora, anebo se obáváte zneužití Vašich osobních údajů?

U této uzavřené otázky volil respondent z odpovědí Důvěřuji – Mám obavu. Svému operátorovi důvěřuje 62,50 % respondentů a 37,50 % má obavy ze zneužití osobních údajů.

16. Přemýšlel(a) jste v případě výhodných předplacených SIM o návratu k této téměř anonymní službě?

Respondent musel zvolit jednu za nabízených odpovědí Ano – Ne. O této možnosti vůbec nepřemýšlí 65,63 % respondentů, nicméně 34,38 % respondentů by využilo možnost výhodných předplacených služeb.

17. Do jaké míry jste spokojen(á) se svým operátorem? Vyznačte jako ve škole.

Respondent měl možnost klasifikace svého operátora dle stupnice jako ve škole Výborný až Nedostatečný. Známkou výborný ohodnotilo 10,94 % respondentů svého operátora, známkou chvalitebný ohodnotilo operátora 35,94 % respondentů, 40,63 % respondentů ohodnotilo známkou dobrý, dostatečný by dalo 10,94 % respondentů a jako nedostatečný, vidí svého operátora 1,56 % respondentů.

18. Jste opatrný(á), chráníte své osobní údaje a informace o Vás, jež je možné zneužít? Vyznačte jako ve škole 1 nejvyšší opatrnost až 5 což je bez obav a opatrnosti.

I u této uzavřené otázky měl respondent možnost oklasifikovat sebe dle stupnice jako ve škole. Na výbornou se oklasifikovalo 10,94 % respondentů, na známku chvalitebně se cítí 31,25 % respondentů, známku dobrý 43,75 % respondentů. Dostatečně se označilo 10,94 % respondentů a jako nedostatečný 3,13 % respondentů.

19. Vaše pohlaví?

Respondent musel zvolit jednu z nabízených odpovědí Muž – Žena. Na tento dotazník odpovědělo 43,75 % mužů a 56,25 % žen.

20. *Kolik je Vám let?*

Každý respondent musel u této otázky uvést svůj věk číslovkou. Odpovědi ukázali, že věk respondentů byl v rozmezí 21 – 76 let.

21. Vzdělání, do jaké skupiny patříte?

Z důvodu nutnosti ukazatele zastoupení respondentů všech skupin vzdělaní, byl respondent nucen vybrat u této uzavřené otázky své dosažené vzdělání. Vysokoškolské

vzdělání uvedlo 53,13 % respondentů, vyšší odborné potvrdilo 7,81 % respondentů, středoškolské s maturitou 28 %, středoškolské bez maturity 1,69 %, dokončené vzdělání vyučen či vyučena uvedlo 7,81 % a základní vzdělání 1,56 % respondentů.

Z výsledku dotazníkového šetření, které proběhlo v období březen až duben 2017 v elektronické i papírové podobě a jehož se zúčastnilo 300 náhodných respondentů, nám vyplývá, že služeb mobilního operátora využívá 100 % z dotazovaných respondentů, z nichž dlouhodobě až 20 let 43,77 % dotazovaných. Dotazník potvrdil i mimo jiné, že stále vedou mezi spotřebiteli skalní operátoři hlavně T-Mobile, což uvedlo 51,56 % respondentů, dále Vodafone 23,44 % a O2 – Telefonica 20,32 %, kdežto služeb virtuálních operátorů využívá téměř zanedbatelné procento respondentů.

Z důvodu ochrany dat a informací je tento dotazník zvláště zaměřen na smluvní spotřebitele mobilních operátorů, neboť předplacené služby jsou provozovány nesmluvně tudíž v podstatě anonymně. Respondenti, jež užívají smluvních neboli paušálních služeb uvedli v 58,62 % (41,38 % neví nebo vůbec nesouhlasili), že souhlasili se zpracováním osobních údajů, z nichž pouhých 19,57 % si je jisto výslovným souhlasem operátorovi se zpracováním svých osobních, identifikační i citlivých údajů. Pouze však zanedbatelné procento respondentů tj. 11,54 % uvedlo, že tyto podmínky četlo, a tak ví, s čím souhlasili. Přesto ale 45,45 % z nich uvedlo, že podmínkám nerozumělo.

Záměrem dotazníkového šetření bylo též zjistit, jak sami respondenti se zajímají o nakládání s jejich osobními daty a informacemi. Respondenti přiznali, že pouhých 9,38 % z nich zajímalo, jak je s jejich daty nakládáno, naopak 90,63 % z nich o tom nikdy nepřemýšlelo a nezajímá je to. Z 85,94 % respondentů užívajících paušálních služeb, uvedlo nízké procento 17,19 % kladnou odpověď informovanost o možnosti písemně požádat mobilního operátora o výpis všech dat, jež o něm mobilní operátor eviduje. Žádný z respondentů však nikdy nevyužil této možnosti oslovení svého operátora tímto způsobem. Stejně tak zanedbatelné procento 15,63 respondentů, ví o možné likvidaci dat po uplynutí zákonné lhůty.

Nicméně i přes tak nízký zájem respondentů o svou ochranu má poměrně vysoké procento přesně 37,50 % obavy z možného zneužití jejich osobních údajů. Přesto lze konstatovat, že respondenti z 87,51 % v podstatě potvrdili spokojenost se svými operátory a pouze malá část z nich 34,38 % by za výhodných podmínek využila téměř anonymní nesmluvní službu předplacených karet.

Pro úplnost tohoto dotazníkového šetření je třeba uvést, že respondenti byli v zastoupení 43,75 % mužů a 56,25 % žen ve věkovém rozpětí 21 – 76 let. Převažovalo zastoupení spíše vzdělaných respondentů a to převážně vysokoškolské vzdělání 53,13 % a středoškolské s maturitou 28 %.

V závěru k tomuto dotazníkovému šetření se zaměřením na ochranu dat a informací u mobilního operátora zvláště se zaměřením na smluvní tudíž paušální spotřebitele, je zřejmě nutné zamyšlení, zda není žádoucí, kromě všech nařízení a novel zákonů na ochranu dat a informací spotřebitele i apelovat přímo na spotřebitele, primárně na jeho větší zájem o vlastní ochranu svých dat a informací. Ať už se jedná o souhlas se zpracováním osobních dat a informací bez přečtení podmínek, jak s nimi bude naloženo, tak i téměř o absolutní nezájem se o svou ochranu starat.

4.6 Anketa

Tato anketa vznikla z důvodu utvoření alespoň přiměřené obrazu, zda lidé mají přehled, co se skrývá pod pojmem „citlivý údaj“. Anketa probíhala 20.03.2017 v odpoledních hodinách v Benešově u Prahy. Bylo osloveno 100 náhodně vybraných dospělých lidí s jedinou otázkou, jež zněla „co si představujete pod pojmem citlivý údaj?“ Z uvedených 100 % dotazovaných odpovědělo 45 %, že se o toto téma nezajímají. Odpověď „nevím“ zazněla u 28 % dotazovaných. Zbylých 27 % odpovědělo následovně na otázku „co si představujete pod pojmem citlivý údaj“:

- Údaje, které jsou úzce spojeny s mou osobou, hlavně rodní číslo i například náboženské vyznání nebo sexuální orientace.
- Údaj, který nechci někomu za daných podmínek sdělit, protože by mě v dalším mohl vážně ohrozit, třeba vydíráním, různými ústrky.
- Údaj, který je zakázán veřejně prezentovat.
- Je to ten údaj, co nechceš, aby věděli ostatní, neměla by je vědět veřejnost, ale jen určitá skupina lidí k tomu určená.
- Tento svět obývám již přes 22 let a mé představy o citlivých údajích směřují k podrobnostem, které mě mohou urážet…sexuální orientace, věk, rasa, váha
- Citlivý údaj, podle toho, kdo se ptá. Když zaměstnavatel, tak třeba zdravotní stav. Pro doktora je to naprosto normální otázka, a zase by se neměl ptát na výši konta. Obecně asi věci víry a svědomí, čemu nebo v co věříš a koho volíš či kolik bereš.
- Třeba údaje o soukromí

- Citlivé údaje jsou to takové údaje, jejichž zveřejněním může člověka poškodit. Domnívám se, že se týkají spíše soukromých věcí člověka.
- Pod pojmem údaj si představuji informaci, která by se neměla dostat každému. Pouze velmi blízkým důvěryhodným osobám, které si sama zvolím.
- Viděl bych to tak, že mezi citlivé věci patří informace o zdravotním stavu, výši příjmů a majetku třeba.
- Není možné dát nějakou universální definici. Je to zkrátka cokoliv, co může být pro nositele informace důležité. Pro někoho je důležité si chránit informaci o velikosti bot a někomu nevadí, že se to o něm šíří. Někdo zase chrání informace o jaderném reaktoru. Tam se shodne asi více lidí, ale třeba takovému příslušníkovi kmene Zulu to je fuk, protože ho to nezajímá.
- Citlivý údaj je údaj (informace), který by měl být zaheslovaný a ke kterému by měli mít přístup jen oprávněné osoby.
- Je to údaj, kterého poskytnutí může nést bezpečnostní riziko jeho zneužití a následné újmy pro subjekt, kterého se údaj týká.
- Je to rozhodně výše mého konta.
- Pod tímto pojmem bych očekávala mou sexuální orientaci.
- Údaj, který tajím i před rodinnými příslušníky.
- Údaj jako je číslo občanského průkazu, protože v případě zneužití tohoto údaje budu mít velké problémy.
- Viděl bych to jako rodné číslo, datum narození a možná i politické zaměření.
- Jednoznačně moje náboženské vyznání.
- Jako citlivý údaj bych si představil cokoliv, ale shrnul bych to na neveřejnou informaci.
- Domnívám se, že pod citlivý údaj patří změna pohlaví, podle mě je to tajná informace kvůli předsudkům a přístupu okolí k takto změněné osobě.
- Určitě to je moje váha jako hmotnost.
- Do citlivého údaje bych zařadil můj etnický původ a možná i moje náboženství.
- Údaj o dosouzení a odpykání trestu.
- Citlivý údaj je každý údaj, který umožní mou identifikaci.
- Údaj, který tajím před všemi.
- Vše o mém soukromí a politickém postoji.

Závěrem z této ankety vyplývá, z větší části, neznalost, popřípadě i nezájem respondentů o ochranu svých citlivých údajů. Pouze část z 27 % respondentů, jež uvedli odpověď, má představu, co to citlivý údaj je. Je tedy otázkou, zda neustálé zdokonalování zákonů a vypracovávání různých Nařízení a Směrnic bude nápomocno, v případě, že sám subjekt, na jehož ochranu je myšleno, se o svou ochranu nestará.

4.7 Řízený rozhovor

Otázky pro řízený rozhovor byly předem připraveny a předloženy Ing. Anně Veverkové, která je jedním z hlavních pracovníků týmu zabývající se bezpečností a ochranou dat a informací ve společnosti T-Mobile Czech Republic a.s. U této společnosti zastává významnou pozici Senior specialista informační a datové bezpečnosti. Každodenně se podílí na neustálém vývoji ochrany, zároveň dohlíží, aby vývoj ochrany informací a dat splňoval náležitosti dle platné právní úpravy.

[1] *Jak dlouho již pracujete v oboru bezpečnosti?*

Od roku 2011 – tj. šestý rok.

[2] *Jaký je Váš názor na stávající právní úpravu?*

Vybírám:

Kybernetická bezpečnost – zákon o kybernetické bezpečnosti – jeví se mi jako dostatečný, v porovnání s ostatními zeměmi relativně pokrokový. Ve velké míře strukturou odpovídá ISO 27001, čili pro ISO certifikované firmy není problém se adaptovat, je to spíš na straně doplnění spousty dokumentace.

Osobní údaje – nyní je pro nás závazná úprava dle zákona 101/2000Sb (o ochraně osobních údajů), ale již probíhá příprava na přechod na úpravu dle nařízení EU GDPR, které vstoupí v účinnost v 5/2018. Tato úprava velmi posiluje postavení subjektu údajů a její požadavky jsou sice teoreticky správné, ale v praxi ve složitém firemním prostředí velmi složité a vyhovět této úpravě nese velké náklady. Navíc slibuje drakonické pokuty pro správce i zpracovatele OsÚ, kteří pochybí, ale přesné výklady o implementaci nejsou, prý přijdou až z praxe…

Zákon o elektronické komunikaci, Krizový zákon, … - musíme vyhovět všem požadavkům, ale ty jsou někdy ne-li přímo proti sobě, tak alespoň jiným směrem. Například každá úprava řeší komunikaci s jinou státní institucí (regulátorem), neexistuje jakákoliv centralizace nebo

komunikace mezi jednotlivými státními institucemi. Pokud bychom tedy v nějakém případě komunikovali s jedním úřadem a druhý opomenuli, stejně pochybíme…

[3] *Je podle Vás dostačující?*

Regulací je v současné době dostatek, jejich smysluplnost a proveditelnost bývá někdy dobrá, ale někdy by se o ní dalo diskutovat. Každopádně bych nepodporovala další regulace, spíše sjednocení požadavků a komunikace s úřady viz výše.

[4] *Spatřujete problém v nedostatečné legislativě,* anebo v *účasti lidského faktoru? Popřípadě proč?*

Největší problém bezpečnosti bývá lidský faktor. Nehledě na zabezpečení a technická či organizační opatření je možné mít významné narušení bezpečnosti od nedbalého nebo škodícího uživatele. V obecné rovině by bylo vhodné pozvednout obecně povědomí o bezpečnosti mezi širokou veřejností. Je-li uživatel neopatrný a nedbá základních bezpečnostních zásad, pak mají útočníci snadnou práci.

[5] *Domníváte se, že dojde díky novému nařízení, jež vstoupí v* platnost v *květnu 2018, ke zlepšení ochrany osobních údajů a informací?*

Budou výrazně posílena práva jednotlivce na ochranu OsÚ, ale z pohledu povinného subjektu je dost komplikované vyhovět a nese to s sebou výrazné náklady. Náš zákon o ochraně osobních údajů byl funkční, ale protože obdobnou úpravu ostatní státy neměly, zasáhla EU. Ochrana informací obecně je na dobré úrovni především u subjektů, které se vydaly cestou ISO certifikace a jiných oborových standardů. GDPR má také mnohem větší záběr co se týká množství povinných subjektů – platí pro všechny >250 zaměstnanců. Zde se povinnosti budou týkat i „menších" firem, které o bezpečnosti zatím vůbec nemají tušení. Čili uvidíme až v praxi.

[6] *Jak vidíte posun ochrany za 5 až 140 let?*

Velkou změnu nepředpokládám – vždy to bude soutěž v rychlosti mezi útočníky a ochránci. Jen se možná změní nástroje a prostředí, ve kterém se bude odehrávat a bude mnohem více informací, které je možné získat a zneužít. Nové technologie se stávají součástí běžného života a stále více se každý z nás stává fyzickým předobrazem svého virtuálního dvojníka (např. internet věcí, vše je v cloudech apod.)

4.8 Podíl mobilních a virtuálních operátorů na trhu v ČR porovnání s dotazníkovým šetřením

Uvedená data počtu uživatelů jsou čerpána z Výročních zpráv mobilních operátorů a data virtuálních operátorů jsou čerpána z nezveřejnitelných interních zdrojů. Zpracování těchto níže uvedených dat je vlastní.

Tabulka č. 1: Počet aktivních SIM karet

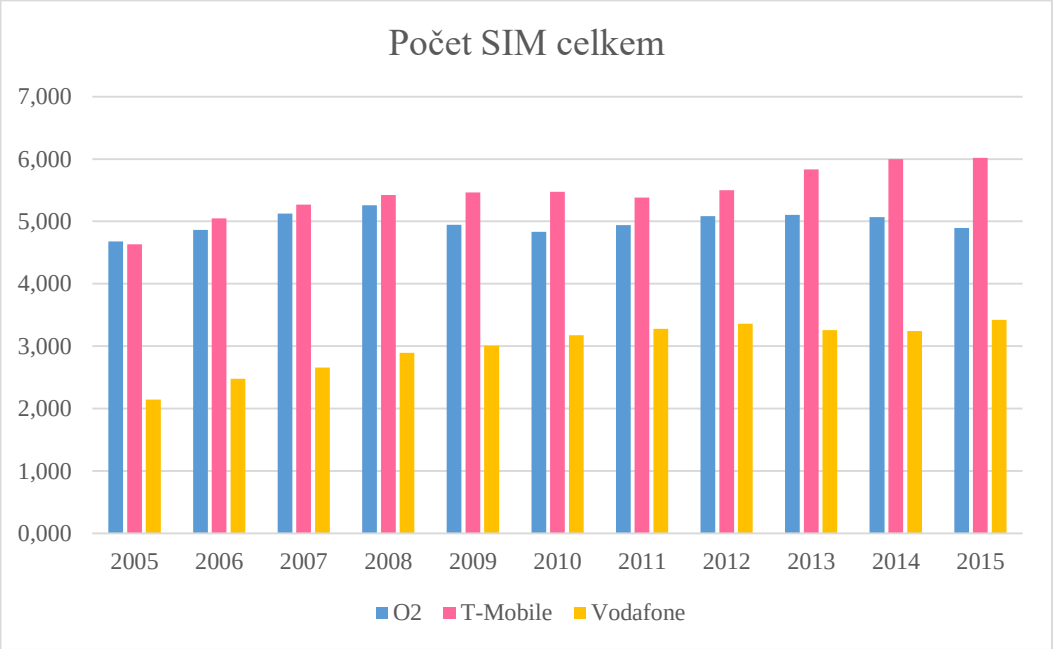
Rok	O2*	T-Mobile*	Vodafone*
2005	4,676	4,634	2,142
2006	4,864	5,049	2,475
2007	5,126	5,271	2,658
2008	5,257	5,422	2,892
2009	4,945	5,464	3,007
2010	4,835	5,475	3,174
2011	4,942	5,381	3,279
2012	5,083	5,498	3,358
2013	5,102	5,831	3,258
2014	5,069	6,000	3,240
2015	4,896	6,019	3,420

*počty aktivních SIM jsou v milionech

Zdroj: vlastní

V uvedené tabulce se jedná o porovnání počtu zákazníků tří mobilních operátorů za období posledních deseti let, a to od roku 2005 do roku 2015. Z tabulky vyplývá, že posledních devět let drží přední pozici v počtu zákazníků společnost T-Mobile. Společnost O2 (tehdy ještě Telefonica) vykazovala nejvyšší počet zákazníků naposledy v roce 2005 a od té doby se počet zákazníků tohoto prvního operátora na českém trhu snižuje. Třetí uvedená společnost Vodafone, jež je z těchto tří uvedených mobilních operátorů nejmladší vykazuje nejnižší počet zákazníků, ale též je zřejmé, že za posledních let pět let u ní nedochází k žádnému poklesu a ani zásadnímu nárůstu počtu zákazníků. Jedná se o stabilní společnost. Tyto data znázorňuje níže uvedený graf:

Graf č. 1: Počet SIM karet



Zdroj: *vlastní*

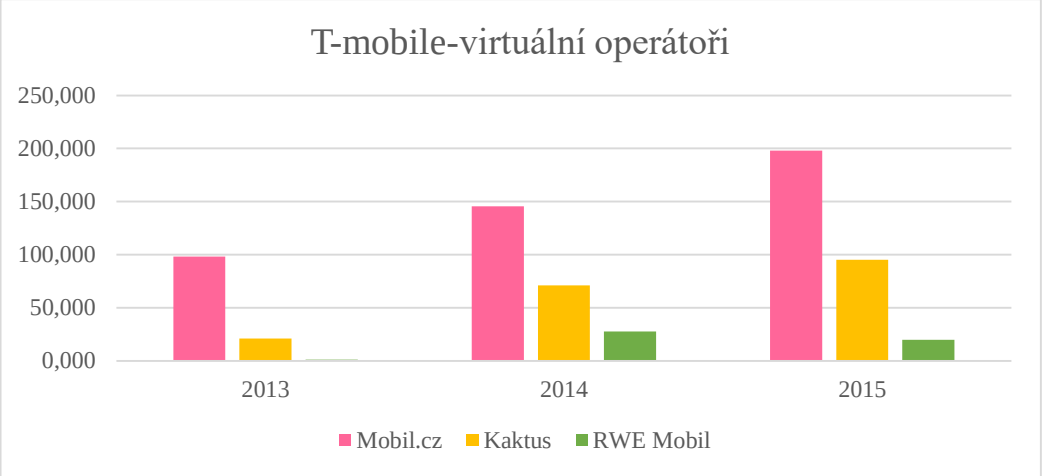
Tito tři hlavní mobilní operátoři zabezpečují pokrytí mobilní sítí v ČR. Od roku 2013 působí nově na českém trhu i virtuální mobilní operátoři, jež nemají vlastní mobilní síť ani infrastrukturu a jejich specifikem je, že ani nevlastní licenci na provozování mobilních sítí udělovanou Českým telekomunikačním úřadem. Tito operátoři vpuštěním na trh Českým telekomunikačním úřadem měli posílit rozvoj maloobchodního konkurenčního trhu, a tím přispět k vyšší ochraně spotřebitele. Virtuální operátoři fungují převážně jako přeprodejci služeb, kteří nabízejí i mnohem méně doplňkových služeb, mezi něž patří i data. Na konci roku 2015 bylo v ČR více jak 100 virtuálních operátorů, avšak nejvýznamnější z nich jsou tito: Blesk mobil, Coop Mobil, Kaktus, Mobil.cz, Mobil od ČEZ, Oskarta, RWE Mobil, Sazka mobil, Tesco Mobile.

Tabulka č. 2: Virtuální operátoři v síti T – mobile

Rok	Mobil.cz	Kaktus	RWE Mobil
2013	98,213	20,933	1,111
2014	145,422	70,940	27,625
2015	198,102	95,086	19,775

Počty aktivních SIM jsou v tis. *Zdroj: vlastní*

Graf č. 2: Virtuální operátoři v síti T – mobile



Zdroj: *vlastní*

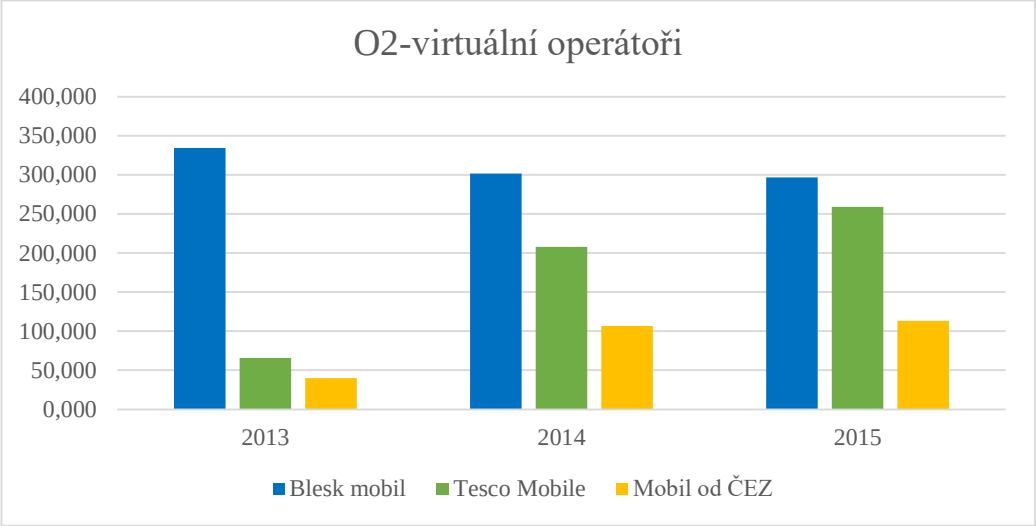
Tabulka č. 3: Virtuální operátoři v síti O2

Rok	Blesk mobil	Tesco Mobile	Mobil od ČEZ
2013	334,400	65,800	40,000
2014	301,400	207,800	106,700
2015	296,600	258,800	113,300

Počty aktivních SIM jsou v tis.

Zdroj: *vlastní*

Graf č. 3: Virtuální operátoři v síti O2



Zdroj *vlastní*

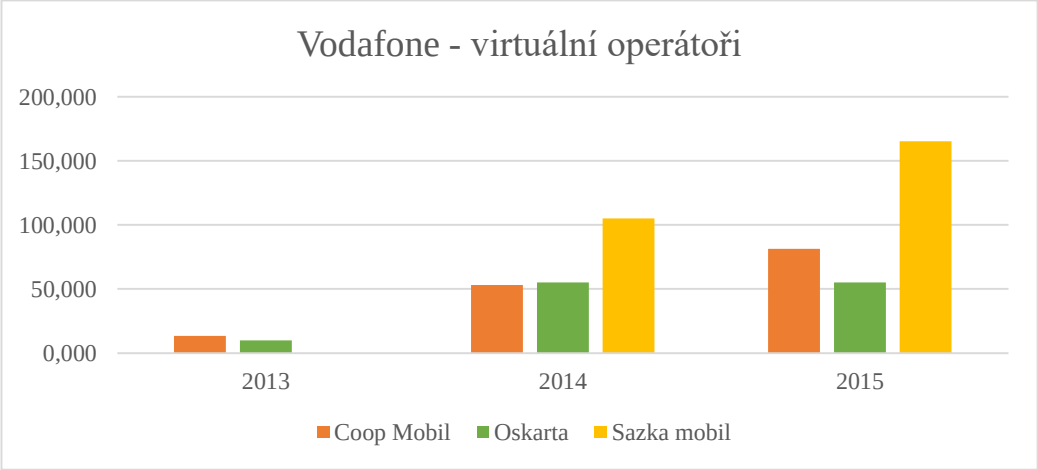
Tabulka č. 4: Virtuální operátoři v síti Vodafone

Rok	Coop Mobil	Oskarta	Sazka mobil
2013	13,300	10,000	0,000
2014	53,000	55,000	105,100
2015	81,400	55,000	165,200

Počty aktivních SIM jsou v tis.

Zdroj: *vlastní*

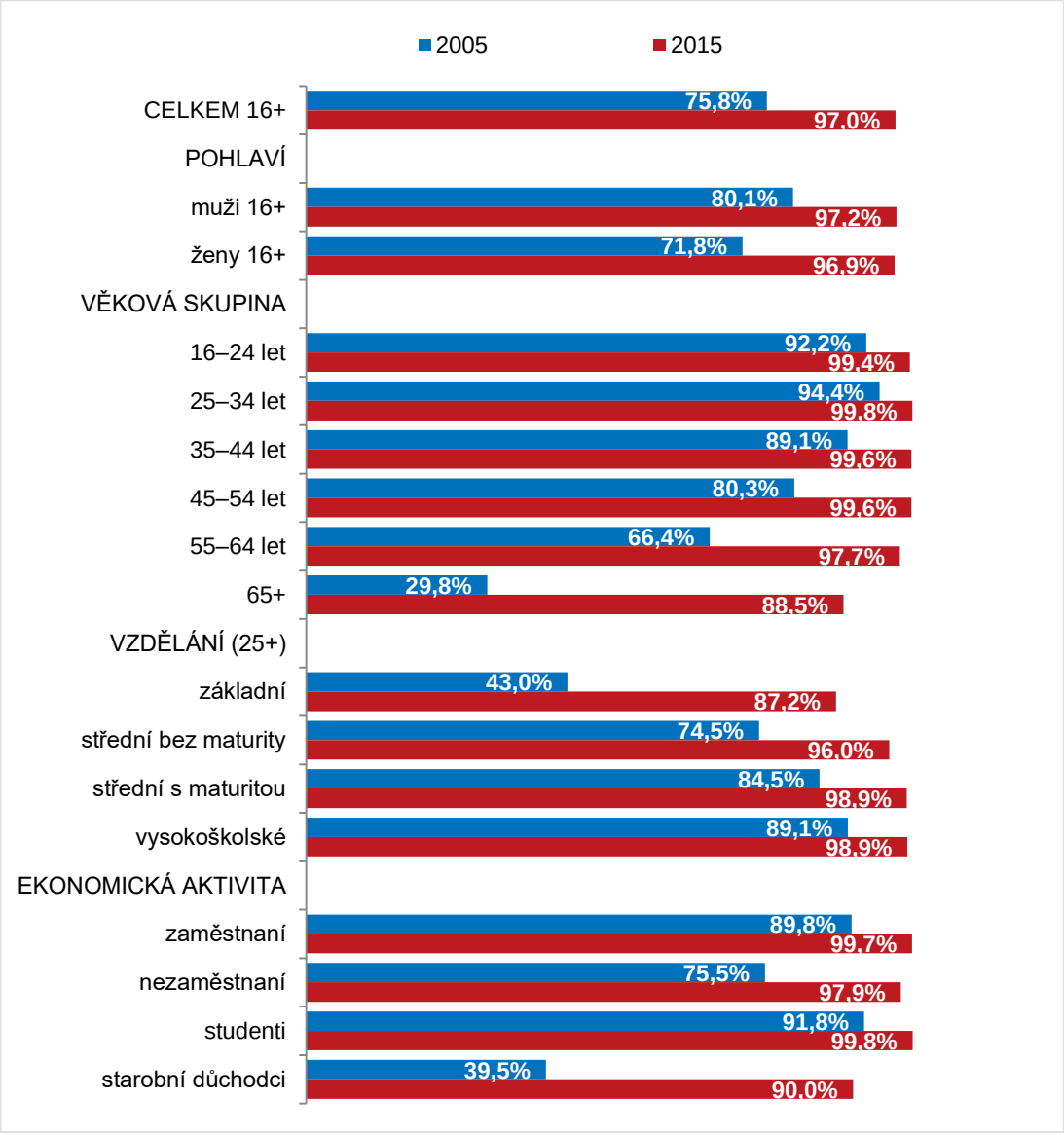
Graf č. 4: Virtuální operátoři v síti Vodafone



Zdroj: *vlastní*

Z dat uvedených v tabulce z porovnání všech tří mobilních operátorů vyplývá, že počet všech zákazníků mobilních operátorů byl v roce 2005 již 11,452 mil. A za dalších deset let se tento počet zvýšil na hranici 14,335 mil. zákazníků, což je nárůst o 2,883 mil., byť bylo očekáváno snížení tohoto počtu z důvodu vstupu virtuálních operátorů na český trh, a to zvláště od roku 2013. Nejsou známa přesná data počtu aktivních SIM karet u všech virtuálních operátorů, ale u devíti výše sledovaných virtuálních operátorů činí tento počet ke konci roku 2015 celkem 1,283 mil. Jedná se o nejvýznamnější virtuální operátory co do počtu zákazníků využívající sítě tří hlavních operátorů.

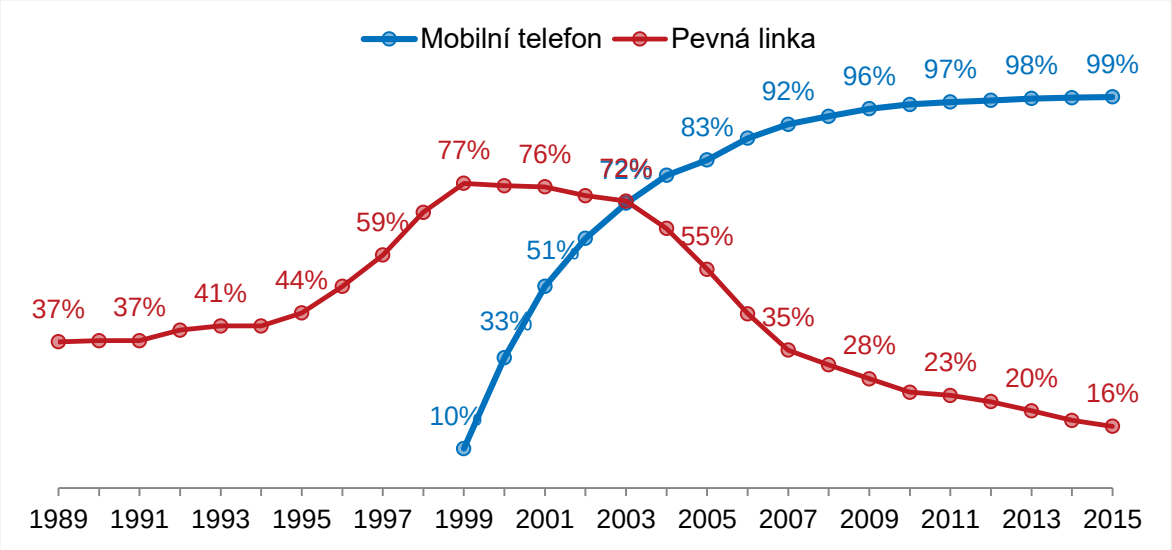
Graf č. 5: Struktura uživatelů mobilních telefonů v ČR (% z celkového počtu jednotlivců v dané socio-demografické skupin)



Zdroj: ČTÚ – VŠIT

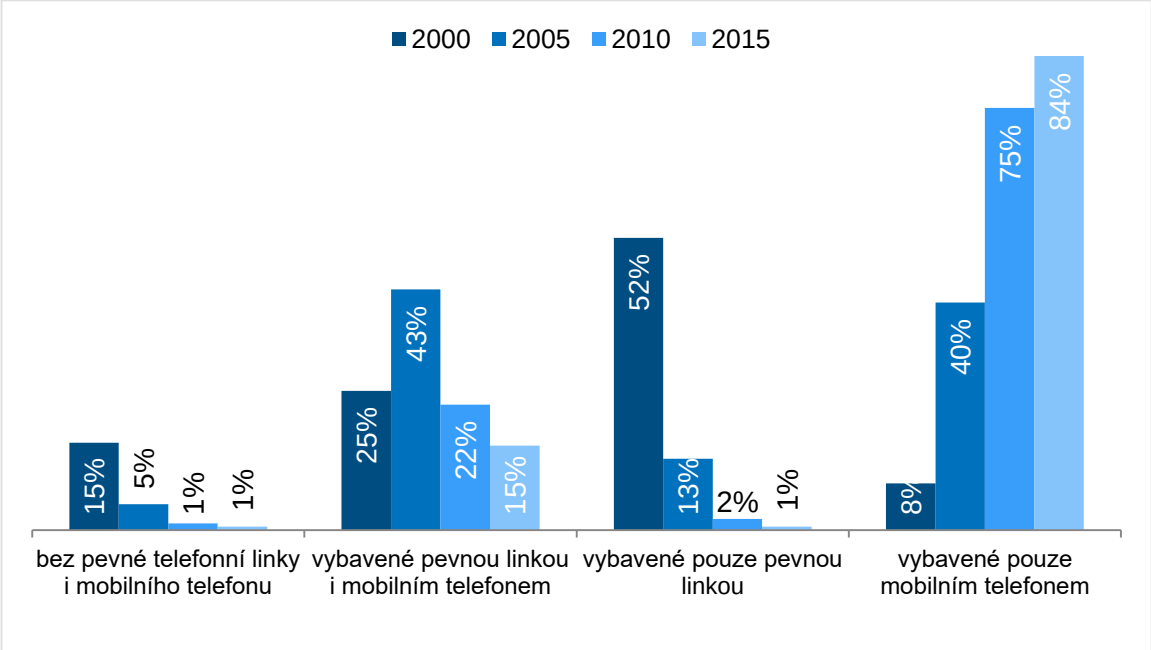
Z tohoto šetření vyplývá, že struktura uživatelů mobilních telefonů je závislá na věku uživatele a šíření mezi starší uživatele je mnohem pomalejší, přesto se děje. V tuto chvíli dochází téměř k nasycení trhu a rozdíly mezi jednotlivými skupinami jsou již minimální a to i zejména z důvodu rušení pevné linky v domácnostech, což znázorňuje níže uvedený graf.

Graf č. 6: Vybavenost domácností telefonem (% z celkového počtu domácností)



Zdroj: ČSÚ, statistika rodinných účtů

Graf č. 7: Vybavenost českých domácností telefony (% z celkového počtu domácností)



Zdroj: ČSÚ, statistika rodinných účtů

5 Poznatky a zhodnocení

Problematika ochrany osobních údajů je dlouhodobě řešená záležitost, dříve na úrovni doporučení a stanovisek ze strany Komise Evropské unie, ale nyní díky neustále se vyvíjejícím technologiím byla Evropská unie nucena řešit tuto ochranu vydáním směrnic (3.1.1.). Základní ochranu osobních údajů zabezpečovala Směrnice Evropského parlament a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Z důvodu zvýšení transparentnosti a tím zamezení možnému zneužívání osobních údajů subjektů včetně posílení práv subjektů, byla vydána Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, jež sjednocuje zvláště předpisy pro zajištění požadované přiměřené ochrany základních práv a svobod. Primárně práva subjektů na soukromí se zaměřením na zpracování osobních údajů v odvětví elektronické komunikace. Odvětví elektronických komunikací bylo doplněno z důvodu sjednocení předpisů pro členské státy, a zvláště z nutnosti úpravy povinností poskytovatelů o Směrnici Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006. Směrnice není vztažena na obsah elektronických komunikací.

Platná právní úprava v souladu s právem Evropského společenství a mezinárodními smlouvami je v České republice regulována zákonem o ochraně osobních údajů č. 101/2000 Sb. a změnou některých zákonů, ve znění účinném od 6. října 2016. Tímto právním předpisem jsou stanoveny cíle a prostředky, jimiž má být dosaženo nejen splnění práva každého na ochranu před protiprávním jednáním jako je zásah do soukromí, ale upravuje i práva a povinnosti při zpracování osobních údajů (3.1.2.). Tento zákon je vztažen na veškeré zpracovávání osobních údajů, ať už se jedná o automatizované zpracování či jiné, kdy automatizované zpracování je bráno jako rizikovější. Zároveň upravuje zpracovateli shromažďování informací a dat o subjektech s ohledem na způsob zpracování a následné zabezpečení tzn., jaké použije standardy a úrovně zabezpečení ochrany osobních údajů subjektů.

Z důvodu neúprosného vývoje a pokroku v technologiích a tím rychlého zastarávání současné právní úpravy na ochranu osobních údajů v EU, a tudíž i v České republice, došlo k vypracování a následnému schválení (podepsání) Evropským parlamentem 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. Pod zkratkou GDPR – General Data Protection Regulation (3.3.3.) vstoupí v účinnost 25. května 2018 ve všech členských státech Evropské Unie. Tímto nařízením bude nahrazena v České republice současná právní úprava ochrany osobních údajů doposud platnou Směrnicí 95/46/ES a zákon 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016. GDPR jednoznačně posiluje práva subjektů nejen v oblasti získávání informací o zpracování svých údajů, ale i v důrazu na vymahatelnost práv subjektů a zároveň ohlašovací povinností správců při jakémkoliv porušení ochrany osobních údajů. Tímto nařízením vzrostou správci i zpracovateli osobních údajů nároky na technická i organizační opatření, jež musí průběžně kontrolovat, čímž se po nich zároveň požaduje i větší samostatná aktivita v tomto směru. Nicméně tyto opatření jsou velmi obdobná těm, které plynou pro mobilního operátora z mezinárodního standardu ISO/IEC 27001:2013, což je certifikace pro řízení bezpečnosti informaci a dále i zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb. i zákonem č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů. Revoluční jsou v tomto nařízení zavedené pokuty za nesplnění povinností. Ty mohou dosáhnout až do výše 20 milionů EUR nebo 4 % z celkového ročního obratu společnosti, vždy bude udělena vyšší možná pokuta. Další zásadní změna pro ochranu osobních údajů, jež vyplývá z nařízení, se týká kategorie citlivé údaje. Nově sem patří genetické a biometrické údaje a zároveň i osobní údaje dětí. Hlavní zásadou v ochraně osobních údajů by měla být minimalizace shromažďování, následná pseudonymizace a transparentnost.

Ochrana osobních údajů v praxi u mobilního operátora společnosti T-Mobile Czech Republic a.s. je zcela v souladu se zákonem č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších přepisů. Operátor má stanovené oprávněné útvary (4.4.1.) a pověřené zaměstnance v souvislosti s oprávněním uvedeným v pracovní smlouvě, jež mohou zpracovávat osobní údaje. Mezi primární způsob zpracování osobních dat u mobilního operátora je shromažďování, uchování, blokování a v poslední řadě likvidace (4.4.2.) osobních údajů. Mobilní operátor jakožto správce osobních údajů podléhá dle zákona Úřadu pro ochranu osobních údajů včetně oznamovací povinnosti. Údaje, jež mobilní operátor zpracovává, jsou hlavně z důvodu smluvních, plnění povinností, pro ověření zletilosti, identity i platební morálky. Cílem mobilního operátora T-Mobile a potažmo celého koncernu Deutsche Telekom je ochrana osobních údajů zákazníků (4.4.3.), což je jeden z hlavních důvodů

neustálých investic do rozvoje technologie napříč celou společností. Snahou je stále větší zjednodušení procesu a tím maximálně omezit přístup k údajům zákazníků, neboť si mobilní operátor plně uvědomuje i ze zkušenosti, že vždy může selhat lidský faktor i při sebelepším zabezpečení.

Pokud se zaměříme na dotazníkové šetření, které proběhlo v elektronické i papírové podobě na téma na téma ochrana osobních dat a informací u mobilního operátora. Tímto šetřením měla být ukázána schopnost respondentů (4.5.), zda vnímají důležitost ochrany svých osobních údajů, jež poskytují svým mobilním operátorům. Na tento dotazník odpovědělo 300 respondentů. Jednalo se zvláště o zaměření na paušální tedy smluvní subjekty, jež využívají služeb mobilního operátora. Hlavním smluvním operátorem byl T-Mobile, jehož uvedlo 51,56 % respondentů jako svého operátora. Ze všech paušálních respondentů tj. 85,94 % uvedlo pouze 58,62 %, že dali souhlas se zpracováním osobních údajů, kdy ostatní respondenti což je 41,38 % neví, anebo souhlas nedali. Nicméně již řadu let je u operátora nemožné bez souhlasu se zpracováním osobních údajů vytvořit platnou smlouvu. Z uvedených 58,62 % respondentů si je jisto 19,57 % výslovným souhlasem operátorovi se zpracováním svých osobních, identifikačních i citlivých údajů. A dále 11,54 % přiznává, že tyto podmínky četli, a tudíž mají představu, s čím souhlasili. Součástí tohoto dotazníkového šetření byl i záměr zjistit, jak sami respondenti se zajímají, jak je nakládáno s jejich osobními údaji. Je až překvapivé zjištění, že pouhých 9,38 % tato problematika zajímala a zbývajících 90,63 % z nich se o tom nikdy nepřemýšlela a nezajímá je to. Nicméně přes tak nízký zájem o svou ochranu má poměrně vysoké procento 37,50 % obavy o možné zneužití svých osobních údajů. Z tohoto šetření vyplývá zásadní otázka, zda je možné chránit někoho, jež sám o svou ochranu nedbá. V podstatě neznalost potvrdil i výsledek ankety (4.6.). Na otázku „co si představujete pod pojmem citlivý údaj“ bylo schopno odpovědět necelých 27 % ze 100 oslovených respondentů. Součástí vlastní práce je porovnání počtu zákazníků hlavních mobilních operátorů včetně virtuálních operátorů. Následně bylo pro přehled a představu, jak velké množství osobních údajů mobilní operátoři zabezpečují a chrání, využito statistik České statistického úřadu, jež nám ukazuje i trend českého trhu výměny tzv. pevných linek za mobilní telefony.

Vzhledem ke stanoveným cílům této práce, čímž bylo seznámení se s problematikou ochrany informací a dat u mobilního operátora, identifikace problému v oblasti ochrany informací a dat u mobilního operátora T-Mobile, je nutné uvést kompletní zhodnocení z vlastního šetření. To znamená, že v návaznosti na výše uvedené dotazníkové šetření, dále osobní šetření ve společnosti T-Mobile, zvláště pak zmapování platné právní

na ochranu osobních údajů, nebylo prokázáno, že by společnost T-Mobile neoprávněně zacházela s osobními údaji.

6 Závěr

Cílem této práce se zaměřením na ochranu osobních údajů u mobilního operátora společnost T-Mobile Czech Republic a.s. bylo nejen seznámení se platnou právní úpravou, jež musí mobilní operátor dodržovat na ochranu údajů svých zákazníků, ale zároveň i zaměření se na mobilního operátora v praxi. Doposud se operátor řídí zvláště zákonem o ochraně osobních údajů č. 101/2000 Sb. a změnou některých zákonů, ve znění účinném od 6. října 2016 (3.1.2.) v součinnosti se Směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracování osobních údajů a o volném pohybu těchto údajů (3.1.1.). Z důvodu větší transparentnosti a posílení práv subjektů byla vydána Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, jež sjednocuje zvláště předpisy pro zajištění požadované přiměřené ochrany základních práv a svobod (3.1.1.). Vzhledem k neustálému rozvoji zvláště využití elektronických komunikací byla v roce 2006 vydána další Směrnici Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006, upravuje zvláště práva spotřebitelů na soukromí a ochranu osobních údajů zvláště v odvětví elektronické komunikace. Mobilní operátor musí z pohledu bezpečnosti a ochrany dodržovat nejen mezinárodní standard ISO/IEC 27001:2013, což je certifikace pro řízení bezpečnosti informaci, ale zároveň podléhá i zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb. (3.3.2.), ale i zákonu č. 127/2005 Sb. o elektronických a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (3.3.1.).

Převratem ve výše zmíněné legislativě má být od 25. května 2018 GDPR – General Data Protection Regulation (3.3.3.) jež vstoupí v účinnost. Jedná se o 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 a zároveň zákon 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016. Mobilní operátor musí mít zavedená technická a organizační opatření na ochranu osobních údajů, ale již teď lze konstatovat, že opatření jsou velmi obdobná výše zmíněnému mezinárodnímu standardu ISO/IEC 27001 i zákonu o kybernetické bezpečnosti stejně tak zákonu o elektronických komunikacích. Nicméně posiluje práva subjektů včetně vymahatelnosti práv subjektů, co týče zpracování

osobních údajů. Určitě však můžeme příchodem GDPR označit jako revoluční sankce, jež budou zavedeny za nesplnění povinností. Pokuty mohou dosáhnout až do výše 20 milionů EUR nebo 4 % z celkového ročního obratu. Každopádně již dnes je bráno každé neoprávněné nakládání s osobními údaji tak, že zakládá trestně právní odpovědnost.

Zaměření na možné problémy v praxi v oblasti ochrany osobních údajů a procesní zpracování (4.4.1., 4.4.2. a 4.4.3), bylo šetřeno přímo u mobilního operátora, kdy postupy nakládání s těmito daty plně potvrdilo součinnost s platnou právní úpravou. Mobilní operátor osobní údaje svých zákazníků maximálně chrání a neustále investuje do rozvoje tohoto zabezpečení napříč celou společností. Mimo jiné spolupracuje i s externím týmem hackerů, čímž neustále zjišťuje možné slabiny svého zabezpečení. Avšak v nedávné době se prokázalo selhání lidského faktoru, kdy se zaměstnanec se pokusil zcizit data zákazníků. Z pohledu Úřadu na ochranu osobní informací došlo k nedostatečnému zabezpečení elektronické interní databáze. Vzhledem k náplni práce tohoto zaměstnance, což byla práce s daty, se jednoznačně jedná o selhání lidského faktoru. Z osobního šetření vyplývá, dokud bude data zpracovávat lidský faktor nelze 100 % zabránit selhání i přes veškeré procesy na ochranu a dokonalé zabezpečení. Zároveň by bylo vhodné apelovat na subjekty, jež své osobní údaje předávají k větší opatrnosti se snahou zvýšit jejich povědomí o ochraně osobních údajů včetně zvýšení právní gramotnosti.

7 Seznam použitých zdrojů

Seznam odborné literatury

Bartík, V., Janečková, E., Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka 3. vydání, Praha: Linde Praha a. s. 2013, 311s. ISBN 978-80-86131-96-2

Bartík, V., Janečková, E., Ochrana osobních údajů v životě podnikatele. 1. vydání edice právo, Nakladatelství ANAG, 2013, 197 s. ISBN 978-80-7263-811-6

Dvořák, Jan – Švestka Jiří a kol.: Občanské právo hmotné 1, díl první: Obecná část, Wolters Kluwer a. s. ČR, 2013, s 430 ISBN 978-80-7478-326-5

ITGP Privacy Team,: The EU General Data Protection Regulation (GDPR): A Practical Guide, Second edition published in the United Kingdom, 400 s., ISBN 978-1-84928-836-1

Hes, A., Regnerová, M., Hrubá, D., Obchodní nauka. Praha: PEF ČZU, 2007 (dotisk). ISBN 80-213-1155-X

Kučerová, A., Nováková, L., a kol.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, 536 s. ISBN 978-80-7179-226-0

Lambert, P., The Data Protection Officer: Proffesion, Rules and Role. 2017 by Taylor and Francis Group, LLC, 300 s., ISBN 978-1-138-03193-7

Maisner, M., Vlachová, B.: Zákon o kybernetické bezpečnosti. Komentář. Praha: Wolters Kluwer, a. s. 2015. 232 s. ISBN 978-80-7478-817-8

Matoušová, M., Hejlík, L.: Osobní údaje a jejich ochrana 2. vydání Praha: ASPI, Wolters Kluwer, 2008, 468s. ISBN 978-80-7357-322-5

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/E

Novák, D.: Zákon o ochraně osobních údajů a předpisy související. Komentář. Praha: Wolters Kluwer, a. s. 2014, 504 s. ISBN 978-80-7478-665-5

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací

Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES,

Švestka, Jiří – Spáčil, Jiří a kol.: Občanský zákoník 1. § 1 až 459. Komentář. 2. vydání. Praha: C. H. Beck, 2009, 1394 s. ISBN 978-80-7400-108-6

Švestka, Jiří – Spáčil, Jiří a kol.: Občanský zákoník 2. § 460 až 880. Komentář. 2. vydání. Praha: C. H. Beck, 2009, 1114 s. ISBN 978-80-7400-108-6

Úmluva o ochraně osob se zřetelem na autorizované zpracování osobních dat č. 108, vyhlášená pod č. 115/2001 Sb.m.s.

Vaníček, Z., Mates, P., Nielsen, T.: Zákon o elektronických komunikacích. Komentář. Praha: Linde Praha a. s., 2014, 560 s. ISBN 978-80-7201-944-1

Zákon č. 40/2009 Sb. trestní zákoník ze dne 8. ledna 2009, ve znění pozdější přepisů
Zákon č. 101/2000 Sb., o ochraně osobních údajů ve znění pozdějších přepisů
Zákon 634/1992 Sb.: o ochraně spotřebitele ze dne 16. prosince 1992, Systém ASPI 9.2.2014 do částky 9/2014 Sb. a 4/2014 Sb.m.s.
Zákon č. 127/2005 sb.: Opatření obecné povahy č. OOP/1/04.2012-4. Česká republika 4.4.2012 ve znění pozdějších přepisů
Zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016
Zákon č. 90/2012 Sb., o obchodních korporacích
Zákon 133/2000 Sb., o evidenci obyvatel
Zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb. A zákona č. 205/2017 Sb.

Seznam internetových zdrojů

iDnes.cz: Ceny redakce Mobil.cz aneb to nejlepší z mobilního roku 2010 [online] Vokáč, Luděk 7.2.2011 [cit. 31.10.2016] Dostupné z: http://mobil.idnes.cz/
iDnes.cz: Mobilní komunikace v České republice zúčtování před ComNetem [online]. 8.6.1997, [cit.24.10.2016] Dostupné z: http://mobil.idnes.cz/mobilni-komunikace-v-ceske-republice-zuctovani-pred-comnetem-pt8-/
iDnes.cz: Ještě letos Telefónica a T-Mobile společně pokryjí většinu Česka LTE [online] ČTK, vse 5.5.2014 [cit. 31.10.2016] Dostupné z: http://mobil.idnes.cz/telefonica-a-o2-sdileji-lte-dcg-/mobilni-operatori.aspx?c=A140505_095129_mobilni-operatori_vse
GDPR - Časť 1: Najzásadnejšie zmeny, ktoré prinesie európska reforma ochrany osobných údajov [online] 5.2.2017 [cit. 27.11.2017] Dostupné z: http://www.steiniger.org/sk/clanky/gdpr-cast-1-najzasadnejsie-zmeny-ktore-prinesie-europska-reforma-ochrany-osobnych-udajov
Ministerstvo vnitra České republiky: Rodné číslo [online 2017] Odbor správních činností, 19. února 2016 [cit. 26.2.2017] Dostupné z: http://www.mvcr.cz/clanek/rady-a-sluzby-dokumenty-rodne-cislo.aspx
Právní prostor: První výkladová pravidla k GDPR, [online] 30.1.2017, Nešpůrek R., [cit. 25.3.2017] Dostupné z: http://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/h-prvni-vykladova-pravidla-k-gdpr
T-Mobile Tiskové centrum: DEUTSCHE TELEKOM KUPUJE ZBÝVAJÍCÍ AKCIE T-MOBILE CZECH REPUBLIC [online] 10.2.2014 [cit. 20.3.2017] dostupné z: https://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/deutsche-telekom-kupuje-zbyvajici-akcie-t-mobile-czech-republic.html
T-Mobile Tiskové centrum: T-Mobile oznamuje úspěšný a inovativní rok [online] 24.2.2016 [cit.31.10.2016] Dostupné z: http://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/t-mobile-oznamuje-uspesny-a-inovativni-rok.html
T-Mobile Tiskové centrum: Milan Vašina generálním ředitelem skupiny Slovak Telekom [online] 23.12.2015 [cit.31.10.2016] Dostupné z: http://www.t-press.cz/cs/tiskove-

materialy/tiskove-zpravy-t-mobile/milan-vasina-generalnim-reditelem-skupiny-slovak-telekom.html
T-Mobile Tiskové centrum: Wi-Fi volání je dostupné pro všechny tarifní zákazníky [online] 31.3.2016 [cit.2.11.2016] Dostupné z: http://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/wi-fi-volani-je-dostupne-pro-vsechny-tarifni-zakazniky.html
T-Mobile Czech Republic a.s., Historie mobilních komunikací, 10. Výročí založení společnosti, Praha 2006, ZRDISC 4424
T-Mobile Czech Republic a.s.: Výroční zpráva 2010, dostupná: http://www.t-mobile.cz/dcpublic/Annual_report_2010_CZ.pdf
T-Mobile Czech Republic a.s.: Výroční zpráva 2011, dostupná: http://www.t-mobile.cz/dcpublic/Annual_report_2011_CZ.pdf
T-Mobile Czech Republic a.s.: Výroční zpráva 2012, http://www.t-mobile.cz/dcpublic/Annual_report_2012_CZ.pdf
T-Mobile Tiskové centrum: T-Mobile: 2013 – Rok plný změn, [online] 6.3.2014 [cit. 31.10.2016] Dostupné z: http://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/t-mobile-2013-rok-plny-zmen.html
T-Mobile Tiskové centrum: 2014: T-Mobile Czech Republic ohlašuje úspěšný rok [online] 26.2.2015 [cit.31.10.216] Dostupné z: http://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/2014-t-mobile-czech-republic-oznamuje-uspesny-rok.html
Úřad pro ochranu osobních údajů: Výroční zpráva 2016, dostupná z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=22715

Magazín

Echo – interní magazín společnosti T-Mobile, registrace: MK ČR E 10161

8 Přílohy

Příloha č. 1: Závazná podniková pravidla pro ochranu soukromí T – mobile

Příloha č. 2: Zpracování cookies společností T – mobile

Příloha č. 3: Podmínky zpracování osobních, identifikačních, provozních a lokalizačních údajů účastníků společnosti T – mobile

Závazná PODNIKOVÁ pravidla Závazná PODNIKOVÁ pravidla pro ochranu SOUKROMÍ při nakládání s osobními údaji v rámci koncernu Deutsche Telekom

Deutsche Telekom AG, oddělení pro ochranu údajů

Verze: 2.7
Datum poslední úpravy: 5. prosince 2013
Stav: finální

Impresum

Editor
Deutsche Telekom AG
Útvar pro ochranu údajů, právní záležitosti a oblast compliance
Oddělení pro ochranu údajů
Friedrich-Ebert-Allee 140, 53113 Bonn, Spolková republika Německo

Název	Verze	Druh dokumentu
Kodex závazných pravidel pro ochranu osobních údajů.docx	2.7	Německo a ostatní země

Autoři	Vydal	Kontaktní osoba
Daniel Hoff Marcus Schmitz. GPR Dr. Jörg Friedrichs, GPR	Manažer oddělení pro ochranu údajů Dr. Claus-Dieter Ulmer	Marcus Schmitz, GPR Dr. Jörg Friedrichs, GPR Stephanie König, GPR

Stav a datum poslední změny	Platnost	Umístění dokumentu
finální 5. prosince 2013	pro Deutsche Telekom AG od 1. července 2014 na základě rozhodnutí představenstva ze dne 10. června 2014. V jednotlivých provozních společnostech v rámci koncernu na základě rozhodnutí představenstva nebo příslušného člena představenstva.	Databáze předpisů DTAG (http:///policies.telekom.de)

Shrnutí
Předpis upravující pravidla pro nakládání s osobními údaji v rámci koncernu. Nová verze Kodexu ochrany osobních údajů.

Historie změn

Verze	Stav ke dni	Editor	Změny / poznámky
2.2	20. ledna 2013	Sonja Klauck	Upravené znění Kodexu ochrany osobních údajů v němčině, verze 2.1
2.3	8. února 2013	Dr. Claus-Dieter Ulmer	Úprava celého znění
2.4	14. února 2013	Dr. Claus-Dieter Ulmer	Předávání údajů a odpovědnost
2.5	21. března 2013	Marcus Schmitz Dr. Claus-Dieter Ulmer	Úprava se zohledněním poznámek německého spolkového komisaře pro ochranu údajů a svobodu informací
2.6	9. dubna 2013	Daniel Hoff	Úprava se zohledněním poznámek německého spolkového komisaře pro ochranu údajů a svobodu informací
2.7	5. prosince 2013	Daniel Hoff Marcus Schmitz	Úprava se zohledněním poznámek rakouského Úřadu na ochranu údajů

Poznámka: Tištěné verze této směrnice koncernu Deutsche Telekom mohou být neaktuální. Informaci o tom, zda se jedná o aktuální verzi směrnice naleznete v databázi předpisů Deutsche Telekom AG na adrese http://policies.telekom.de.

OBSAH

Úprava se zohledněním poznámek rakouského Úřadu na ochranu údajů ... 2
Část I Rozsah platnosti ... 6
Článek 1 Právní povaha Kodexu závazných pravidel pro ochranu údajů ... 6
Článek 2 Rozsah platnosti ... 6
Článek 3 Vztah k jiným právním předpisům ... 6
Článek 4 Vypršení a ukončení platnosti ... 7
Část II Zásady ... 8
Oddíl 1 Transparentnost zpracování údajů ... 8
Článek 5 Informační povinnost ... 8
Článek 6 Obsah a forma informací ... 8
Článek 7 Dostupnost informací ... 8
Oddíl 2 Podmínky pro použití osobních údajů ... 9
Článek 8 Princip ... 9
Článek 9 Podmínky pro použití osobních údajů ... 9
Článek 10 Souhlas ze strany subjektu údajů ... 9
Článek 11 Automatizovaná individuální rozhodnutí ... 9
Článek 12 Použití osobních údajů pro účely přímého marketingu ... 10
Článek 13 Citlivé údaje ... 10
Článek 14 Přiměřenost, zpracování údajů pouze v nutných případech, anonymizace a využití pseudonymů ... 10
Článek 15 Zákaz podmiňování poskytnutí služeb souhlasem k použití údajů ... 10
Oddíl 3 Předávání osobních údajů ... 10
Článek 16 Povaha a účel předávání osobních údajů ... 10
Článek 17 Předávání údajů ... 11
Článek 18 Zpracovávání údajů dodavateli ... 11
Oddíl 4 Kvalita a bezpečnost údajů ... 11
Článek 19 Kvalita údajů ... 11
Článek 20 Bezpečnost údajů – technická a organizační opatření ... 12
Část III Práva subjektů údajů ... 13
Článek 21 Právo na informace ... 13
Článek 22 Právo na vznesení námitky, právo na vymazání či zablokování údajů a právo na opravu ... 13
Článek 23 Právo na vysvětlení, komentář a zjednání nápravy ... 13
Článek 24 Právo na dotazy a stížnosti ... 14
Článek 25 Výkon práv subjektů údajů ... 14
Článek 26 Písemná kopie Kodexu závazných pravidel pro ochranu údajů ... 14
Část IV Řízení procesu ochrany údajů ... 15
Článek 27 Odpovědnost za zpracování údajů ... 15
Článek 28 Zmocněnec odpovědný za ochranu údajů ... 15
Článek 29 Zmocněnec odpovědný za ochranu údajů v rámci koncernu Deutsche Telekom ... 15
Článek 30 Informační povinnost v případě porušení ... 16
Článek 31 Kontrola úrovně ochrany údajů ... 16

Článek 32 Zavázání a proškolení zaměstnanců 17
Článek 33 Spolupráce s příslušnými orgány dozoru 17
Článek 34 Osoby odpovědné za vyřizování dotazů 17
Část IV Odpovědnost 18
Článek 35 Rozsah platnosti pravidel upravujících odpovědnost 18
Článek 36 Poskytovatel náhrady 18
Článek 37 Důkazní břemeno 18
Článek 38 Subjekt údajů jako dotčená osoba 18
Článek 39 Jurisdikce 18
Článek 40 Mimosoudní rozhodčí řízení 19
Část VI Závěrečná ustanovení 20
Článek 41 Revize a úpravy tohoto Kodexu závazných pravidel pro ochranu údajů 20
Článek 42 Seznam kontaktních osob a společností 20
Článek 43 Procesní právo / oddělitelnost 20
Článek 44 Zveřejnění 20
Část VII Definice pojmů 21

Poznámka:

V případě, že tato závazná Pravidla budou implementována v jednotlivých společnostech na základě individuálních předpisů, je nutné dodržet ujednání všech stávajících kolektivních smluv i rozhodovací práva příslušných orgánů zastupujících zaměstnance.

ÚVOD

(1) Ochrana osobních údajů zákazníků, zaměstnanců a jiných osob, které mají s koncernem Deutsche Telekom jakýkoli vztah, je pro společnosti v rámci koncernu Deutsche Telekom jednou z hlavních priorit.

(2) Společnosti v rámci koncernu Deutsche Telekom si jsou vědomy, že úspěch koncernu Deutsche Telekom jako celku závisí nejen na globálním propojení informačních toků, ale především na důvěryhodném a bezpečném nakládání s osobními údaji.

(3) V řadě oblastí vnímají zákazníci i veřejnost koncern Deutsche Telekom jako jediný subjekt. Společným zájmem společností v rámci koncernu Deutsche Telekom proto je významně přispět ke společnému úspěchu a zavedením těchto Pravidel podpořit cíl koncernu Deutsche Telekom, jímž je poskytování produktů a služeb vysoké kvality.

(4) Přijetím těchto Pravidel vytváří koncern Deutsche Telekom jednotnou úpravu ochrany údajů na vysoké úrovni, která platí po celém světě pro nakládání s údaji jak v rámci jednotlivých společností, tak mezi jeho jednotlivými společnostmi navzájem, pro předávání údajů v rámci Spolkové republiky Německo i v zahraničí. V rámci koncernu Deutsche Telekom musí být zajištěno, že příjemce osobních údajů bude tyto údaje zpracovávat v souladu se zásadami upravenými v právních předpisech na ochranu údajů, jež se vztahují na jejich odesilatele.

I.ROZSAH PLATNOSTI

1. Právní povaha Pravidel

Tato Pravidla upravují oblast zpracovávání osobních údajů (v souladu s pracovním dokumentem 133 pracovní skupiny Evropské komise zřízené podle článku 29) ve všech provozních společnostech v rámci koncernu Deutsche Telekom, které jej přijaly jako závazný předpis. Pravidla jsou rovněž závazná pro všechny společnosti, kde bude Deutsche Telekom jeho přijetí vyžadovat, jakož i pro všechny společnosti, které jej přijaly dobrovolně, a to bez ohledu na to, kde jsou údaje shromažďovány.

2. Rozsah platnosti

Pravidla platí ve vztahu k použití všech druhů osobních údajů v rámci koncernu Deutsche Telekom, bez ohledu na to, kde jsou údaje shromažďovány. Osobní údaje se v rámci koncernu Deutsche Telekom používají zejména pro následující účely:

(1) Správa zaměstnaneckých osobních údajů při sjednávání, plnění a zpracovávání pracovních smluv a oslovování zaměstnanců ze strany koncernu Deutsche Telekom nebo třetích stran za účelem nabídky produktů a služeb.

(2) Sjednávání, plnění a zpracovávání smluv uzavíraných se zákazníky – podnikateli i spotřebiteli, a provádění činností v oblasti reklamy a průzkumu trhu, jejichž cílem je informovat zákazníky a zájemce z řad třetích stran o produktech a službách nabízených koncernem Deutsche Telekom či třetími stranami.

(3) Sjednávání a plnění smluv s dodavateli koncernu Deutsche Telekom v rámci poskytování služeb pro koncern Deutsche Telekom.

(4) Jednání se třetími stranami, zejména akcionáři, partnery či návštěvníky a dodržení závazných právních předpisů.

Údaje mohou být používány výhradně v souladu se stávajícím a budoucím předmětem podnikání společností v rámci koncernu Deutsche Telekom, který zahrnuje poskytování telekomunikačních služeb, digitálních služeb pro zákazníky – spotřebitele i podnikatele, IT služeb (včetně služeb datových center) a poradenství.

3. Vztah k jiným právním předpisům

(1) Cílem ustanovení Pravidel je zajistit vysoký stupeň ochrany údajů, a to jednotně pro celý koncern Deutsche Telekom. Těmito Pravidly však nejsou dotčeny žádné stávající povinnosti ani předpisy, kterými se při zpracovávání a použití osobních údajů musí řídit jednotlivé společnosti, jež jdou nad rámec níže uvedených zásad či která obsahují další omezení ohledně zpracovávání a použití osobních údajů.

(2) Údaje shromážděné v Evropě mohou být obecně použity výhradně v souladu s právními předpisy země, v níž byly shromážděny, a to bez ohledu na skutečnost, kde dochází k jejich použití, avšak minimálně v souladu s požadavky stanovenými v těchto Pravidlech.

(3) Těmito Pravidly není dotčena platnost právních předpisů jednotlivých zemí upravujících státní bezpečnost, obranu státu nebo veřejný pořádek či přijatých za účelem prevence kriminality a vyšetřování trestných činů a pachatelů trestné činnosti, na základě nichž se vyžaduje předávání údajů třetím stranám. V případě, že určitá provozní společnost zjistí, že významná část těchto Pravidel je v rozporu s právními předpisy dané země

upravujícími ochranu osobních údajů, v důsledku čehož nebudou moci příslušné strany tato Pravidla podepsat, vyrozumí o tom neprodleně zmocněnce odpovědného za ochranu osobních údajů v rámci koncernu Deutsche Telekom (*Group Data Privacy Officer*). Na procesu řešení této záležitosti se pak jako mediátor bude podílet příslušný orgán dozoru nad danou společností.

4. Vypršení a ukončení platnosti

Tato Pravidla pozbývají platnosti vůči jednotlivé společnosti, pokud tato přestane být členem koncernu Deutsche Telekom nebo pokud rozhodne o neplatnosti pravidel v něm upravených. Vypršením či ukončením platnosti těchto Pravidel však není příslušná společnost zbavena svých povinností a/nebo závazků Pravidel pro ochranu údajů upravujících používání již předaných údajů. Další údaje mohou být této společnosti či touto společností předány pouze v případě, že poskytne příslušné procesní záruky, které budou v souladu s požadavky evropského práva.

II. Zásady
Oddíl 1
TRANSPARENTNOST ZPRACOVÁNÍ ÚDAJŮ

5. Informační povinnost

Subjekty údajů musí být informovány o tom, jak jsou jejich osobní údaje používány v souladu s příslušnými právními předpisy a níže uvedenými podmínkami.

6. Obsah a forma informací

(1) Příslušná společnost musí subjektům údajů náležitým způsobem poskytnout následující informace:

a) informace o identitě správce (správců) údajů a jeho (jejich) kontaktní informace;

b) informace o zamýšleném použití údajů a účelu jejich použití. Tyto informace by měly zahrnovat bližší určení toho, jaké údaje se zaznamenávají, příp. zpracovávají/používají, proč, za jakým účelem a na jakou dobu;

c) v případě, že jsou osobní údaje předávány třetím stranám, musí být také známy informace o příjemci, rozsahu a účelu (účelech) jejich předání;

d) informace o právech subjektů údajů, které jim náleží v souvislosti s použitím údajů o nich.

(2) Bez ohledu na zvolené médium musí být tyto informace subjektům údajů poskytnuty v jasné a srozumitelné formě.

7. Dostupnost informací

Výše uvedené informace musí být subjektům údajů poskytnuty při jejich prvním shromáždění a následně při každém dalším vyžádání.

ODDÍL 2
PODMÍNKY PRO POUŽITÍ OSOBNÍCH ÚDAJŮ

8. Zásada

Osobní údaje mohou být použity pouze za níže uvedených podmínek a nesmí být použity pro jiné účely, než pro něž byly původně shromážděny.

Shromážděné údaje mohou být použity pro jiné účely pouze v případě splnění níže uvedených podmínek.

9. Podmínky pro použití osobních údajů

Osobní údaje mohou být použity, pokud je splněno jedno či více následujících kritérií:

a) Použití údajů zamýšleným způsobem je z právního hlediska jasně přípustné.

b) Subjekt údajů poskytl souhlas s použitím jeho údajů.

c) Použití dat daným způsobem je nezbytné k tomu, aby příslušná společnost mohla plnit své povinnosti vyplývající ze smlouvy se subjektem údajů, včetně své smluvní informační povinnosti a/nebo sekundárních povinností, nebo aby daná společnost mohla realizovat opatření vyžadovaná před uzavřením smlouvy či po jejím uzavření související se sjednáním nebo zpracováním smlouvy, která si vyžádal subjekt údajů.

d) Použití údajů je nutné ke splnění zákonných povinností společnosti.

e) Použití údajů je nezbytné k zajištění podstatných zájmů subjektu údajů.

f) Použití údajů je nutné k provedení úkonu, který je v zájmu veřejnosti nebo který je součástí výkonu veřejné moci a jehož provedením byla daná společnost nebo třetí strana, jíž byly údaje předány, pověřena.

g) Zpracování údajů je nutné k výkonu oprávněných zájmů společnosti nebo třetí strany (třetích stran), jíž (jimž) byly údaje předány, pokud nad těmito zájmy jasně nepřeváží zájmy subjektu údajů na zaručení ochrany údajů.

10. Souhlas ze strany subjektu údajů

Má se za to, že subjekt údajů poskytl svůj souhlas podle čl. 9 odst. 1 bod b) těchto Pravidel, pokud:

a) Jde o o souhlas výslovný, dobrovolný a informovaný tak, aby bylo subjektu údajů zřejmé, v jakém rozsahu souhlas poskytuje. Znění prohlášení o souhlasu musí být dostatečně určité a musí subjekt údajů informovat o jeho právu vzít tento souhlas kdykoli zpět. Subjekt údajů musí být informován o případech, kdy má zpětvzetí za následek neplnění smluvních podmínek.

b) Byl souhlas získán v podobě přiměřené okolnostem (v písemné podobě). Ve výjimečných případech může jít o souhlas ústní, pokud je dostatečně doloženo jeho poskytnutí a okolnosti, z nichž vyplývá, že ústní souhlas je postačující.

11. Automatizovaná individuální rozhodnutí

a) Rozhodnutí, která hodnotí jednotlivé aspekty určité osoby a mohou s sebou pro takovouto osobu nést právní důsledky či na ni mohou mít značný negativní vliv, nesmí být založena pouze na automatizovaném použití údajů. To se týká zejména rozhodnutí, pro něž jsou důležité údaje o bonitě, odborné způsobilosti či zdravotním stavu subjektu údajů.

b) Pokud bude v individuálních případech automatizované rozhodnutí objektivně nutné, bude subjekt údajů o jeho výsledku neprodleně informován a bude mu poskytnuta příležitost se k němu v přiměřené časové lhůtě vyjádřit. Vyjádření subjektu údajů bude před přijetím finálního rozhodnutí vzato přiměřeným způsobem v úvahu.

12. Použití osobních údajů pro účely přímého marketingu

V případě použití údajů pro účely přímého marketingu subjekty údajů:

a) musí být informovány o způsobu použití jejich údajů pro účely přímého marketingu;

b) musí být informovány o svém právu kdykoli odmítnout použití svých osobních údajů pro účely přímého marketingu; a

c) musí mít k dispozici nástroje k uplatnění svého práva odmítnout přijímání takových sdělení. Musí být zejména informovány o tom, komu mohou takové odmítnutí adresovat.

13. Citlivé údaje

a) Použití citlivých osobních údajů je povoleno pouze tehdy, umožňují-li to právní předpisy nebo k tomu dal subjekt údajů svůj předchozí souhlas. Použití citlivých osobních údajů je rovněž povoleno, je-li nutné pro zpracování osobních údajů za účelem naplnění práv a splnění povinností příslušné společnosti v oblasti pracovního práva, byla-li přijata přiměřená opatření na ochranu takových osobních údajů a nezakazuje-li to právo daného státu.

b) Před zahájením shromažďování, zpracovávání či použití takovýchto údajů je příslušná společnost povinna vyrozumět zmocněnce odpovědného za ochranu osobních údajů a takový úkon zdokumentovat. Při posuzování přípustnosti shromažďování, zpracovávání či použití údajů by měla být zejména zohledněna povaha, rozsah, účel, nutnost a právní důvod použití údajů.

14. Přiměřenost, zpracování osobních údajů pouze v nutných případech, anonymizace a využití pseudonymů

(1) Osobní údaje musí být s ohledem na jejich použití pro konkrétní účel přiměřené, relevantní a musí mít odpovídající rozsah (přiměřenost). V rámci konkrétního využití smí být osobní údaje zpracovávány pouze tehdy, je-li to nutné (zpracování údajů pouze v nutných případech).

(2) V případech, kdy je to možné a ekonomicky opodstatněné, je třeba aplikovat procesy pro vymazání identifikačních znaků subjektů údajů (anonymizace) či jejich nahrazení jinými charakteristikami (využití pseudonymů).

15. Zákaz podmiňování poskytnutí služeb souhlasem k použití údajů

Využívání služeb nebo poskytování produktů a/nebo služeb nesmí být podmiňováno poskytnutím souhlasu ze strany subjektu údajů k použití jeho údajů pro jiné účely než sjednání či plnění příslušné smlouvy. To platí pouze v případě, že subjekt údajů nemá možnost nebo nemá přiměřenou možnost využívat srovnatelné služby nebo srovnatelné produkty.

ODDÍL 3
PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ

16. Povaha a účel předávání osobních údajů

(1) Osobní údaje mohou být předávány pouze v případě, že jejich příjemce převezme odpovědnost za předané údaje (předání) nebo že příjemce

použije údaje výhradně v souladu s pokyny a požadavky jejich odesilatele (smlouva o zpracování údajů).

(2) Osobní údaje lze předávat pouze pro povolené účely dle čl. 9 těchto Pravidel v rámci výkonu podnikání dané společnosti nebo plnění jejích zákonných povinností či na základě souhlasu poskytnutého subjekty údajů.

17. Předávání údajů

(1) V případě, že jednotlivá společnost předává údaje subjektům, které mají hlavní provozovnu v jiné zemi, nebo se jedná o přeshraniční předávání údajů, musí být provedena opatření, jejichž cílem je zajistit řádné předání údajů. S příjemcem údajů musí být ještě před předáním údajů sjednány přiměřené požadavky na zajištění ochrany a bezpečnosti údajů. Osobní údaje, zejména osobní údaje shromážděné v zemích Evropské unie či Evropského hospodářského prostoru, mohou být předány zpracovatelům mimo Evropskou unii pouze za předpokladu, že bude zajištěna přiměřená ochrana osobních údajů v souladu s těmito Pravidly nebo budou přijata jiná přiměřená opatření, např. standardní smluvní doložky používané v rámci EU nebo individuální smluvní ujednání splňující příslušné požadavky evropského práva.

(2) Na základě požadavků koncernu Deutsche Telekom a obecně uznávaných technických a organizačních standardů musí být přijata náležitá technická a organizační opatření, která zaručí bezpečnost osobních údajů, zejména při jejich předávání třetí straně.

18. Zpracovávání údajů dodavateli[1]

(1) V případě, že společnost (objednatel) pověří třetí stranu (dodavatele), aby za objednatele poskytoval určité služby v souladu s jeho pokyny, musí smlouva o poskytování služeb kromě ujednání specifikujícího plnění, které má dodavatel poskytnout, rovněž obsahovat povinnosti dodavatele jakožto strany pověřené zpracováním údajů. Tyto povinnosti musí obsahovat pokyny objednatele ohledně druhu a způsobu zpracování osobních údajů, účelu jejich zpracování a technických a organizačních opatřením potřebných pro jejich ochranu.

(2) Dodavatel není bez předchozího souhlasu objednatele oprávněn použít osobní údaje (které mu byly svěřeny za účelem provedení zakázky) pro vlastní zpracovatelské účely či zpracovatelské účely třetích stran. Dodavatel je povinen předem informovat objednatele o úmyslu zadat plnění zakázky, která je předmětem smlouvy uzavřené s objednatelem, třetím stranám. Objednatel má právo nesouhlasit s využitím třetích stran při plnění zakázky. V případě, že jsou k plnění zakázky přípustným způsobem využity subdodavatelé, je dodavatel povinen zavázat je k plnění požadavků stanovených ve smlouvě uzavřené mezi dodavatelem a objednatelem.

(3) Subdodavatelé budou vybráni podle schopnosti splnit výše uvedené požadavky.

ODDÍL 4
KVALITA A BEZPEČNOST ÚDAJŮ

19. Kvalita údajů

(1) Osobní údaje musí být správné a v případě nutnosti musí být průběžně aktualizovány (kvalita údajů).

(2) S ohledem na účel, k němuž mají být údaje použity, musí být přijata náležitá opatření, aby bylo zajištěno vymazání, zablokování či případně oprava jakýchkoli nesprávných či neúplných informací.

20. Bezpečnost údajů – technická a organizační opatření. Jednotlivé společnosti jsou povinny přijmout náležitá technická a organizační opatření ve vztahu k interním procesům, IT systémům a platformám využívaným při shromažďování, zpracovávání a používání údajů za účelem jejich ochrany.

Tato opatření musí:

a) zabránit přístupu neoprávněných osob k systémům pro zpracování údajů, v rámci nichž jsou zpracovávány či používány osobní údaje (regulace fyzického přístupu);
b) zajistit, aby neoprávněné osoby nemohly systémy pro zpracování údajů používat (regulace používání datových systémů);
c) zajistit, aby osoby oprávněné k používání systému pro zpracování údajů měly přístup výhradně k údajům, k nimž jsou oprávněny přistupovat, a aby neoprávněné osoby nemohly osobní údaje během zpracovávání či používání či po jejich zaznamenání číst, kopírovat, měnit ani mazat (regulace přístupu k údajům);
d) zajistit, aby v průběhu elektronického přenosu či předávání či nahrávání údajů na datový nosič nemohly

[1] Tento článek není ustanovením ve smyslu pracovního dokumentu 195 pracovní skupiny zřízené Evropskou komisí podle článku 29.

neoprávněné osoby osobní údaje číst, kopírovat, měnit ani mazat a aby bylo možné prověřit a identifikovat zpracovatele, jimž mají být údaje přenášeny prostředky pro přenos dat (regulace přenosu dat);

e) zajistit, aby bylo možné zpětně přezkoumat a zjistit, zda a kým byly osobní údaje do systémů pro zpracovávání údajů zadány, v těchto systémech změněny či z nich vymazány (kontrola zadávání údajů);

f) zajistit, aby osobní údaje zpracovávané dodavateli byly zpracovávány pouze v souladu s pokyny objednatele (kontrola dodavatele);

g) zajistit ochranu osobních údajů proti náhodnému zničení či ztrátě (zajištění dostupnosti údajů);

h) zajistit, aby údaje shromážděné pro různé účely byly zpracovávány odděleně (pravidlo odděleného zpracování údajů).

III. PRÁVA SUBJEKTŮ ÚDAJŮ

21. Právo na informace

(1) Každý subjekt údajů má právo kdykoli kontaktovat jakoukoli společnost, která používá jeho údaje, a požadovat poskytnutí informací týkajících se:

a) osobních údajů o ní uložených, včetně jejich původu a příjemce (příjemců);

b) účelu jejich použití;

c) osob a zpracovatelů, kterým jsou jejich údaje standardně předávány, zejména v případě jejich předávání do zahraničí;

d) ustanovení těchto Pravidel.

(2) Tyto informace by měly být příslušnému žadateli, který o ně projeví zájem, sděleny ve srozumitelné podobě a v přiměřené časové lhůtě, a to obecně v písemné či elektronické podobě. Poskytnutí písemné kopie těchto Pravidel se považuje za dostatečný způsob sdělení informací o požadavcích v něm upravených.

V případech, kdy to příslušné právní předpisy dané země dovolují, si může společnost za poskytnutí příslušné informace účtovat poplatek.

22. Právo na vznesení námitky, právo na vymazání či zablokování údajů a právo na opravu

(1) Subjekt údajů může kdykoli vznést námitku proti použití jeho údajů, pokud se údaje používají k účelu, který není právně závazný.

(2) Toto právo na vznesení námitky platí i v případě, že subjekt údajů dal k použití jeho údajů předchozí souhlas.

(3) Oprávněné žádosti o výmaz či zablokování údajů musí být neprodleně kladně vyřízeny. Takovéto žádosti jsou oprávněné zejména tehdy, pominou-li právní důvody pro použití údajů. Má-li subjekt údajů na výmaz údajů právo, ale není-li výmaz možný nebo není možný při vynaložení přiměřeného úsilí, budou údaje chráněny proti nepovolenému užití jejich zablokováním, přičemž budou dodrženy zákonné lhůty pro uchování údajů.

(4) Subjekt údajů může kdykoli požádat, aby příslušná společnost opravila jeho osobní údaje evidované takovou společností v případě, že tyto údaje jsou neúplné a/nebo nesprávné.

(5) Subjekt údajů musí být informován o případech, kdy má zpětvzetí nebo výmaz údajů za následek neplnění smluvních podmínek.

23. Právo na vysvětlení, komentář a zjednání nápravy

(1) V případě tvrzení subjektu údajů, že byla porušena jeho práva v důsledku nezákonného použití jeho údajů, zejména pak v případě předložení důkazů o prokazatelném porušení těchto Pravidel , jsou dotčené společnosti povinny bez zbytečného odkladu zjistit okolnosti případu. Zejména v případě předání či přenosu údajů společnostem mimo Evropskou unii je společnost se sídlem v Evropské unii povinna zjistit okolnosti případu a prokázat, že příjemce požadavky stanovené v těchto Pravidlech neporušil nebo že je odpovědný za způsobenou újmu. Dotčené společnosti spolu budou úzce spolupracovat a vzájemně si umožní přístup ke všem informacím, jež jsou nezbytné za účelem zjištění okolností případu.

(2) Dotčený subjekt údajů je oprávněn kdykoli podat stížnost na holdingovou společnost koncernu Deutsche Telekom, má-li za to, že určitá společnost v rámci koncernu Deutsche Telekom nezpracovává jeho osobní údaje v souladu s požadavky právních předpisů nebo ustanoveními těchto Pravidel . Důvodné stížnosti budou vyřízeny v řádné lhůtě a subjekt údajů bude o výsledku vyrozuměn.

(3) V případě, že se stížnost týká několika společností, bude pracovník odpovědný za ochranu osobních údajů ve společnosti, která je nejlépe obeznámena s předmětem stížnosti, koordinovat veškerou příslušnou korespondenci se subjektem údajů. Pracovník odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom je oprávněn kdykoli uplatnit své právo na subrogaci a převzetí daného případu do své kompetence.

(4) Musí být zavedeny náležité kanály pro oznamování případů porušení práv na ochranu osobních údajů (např. speciální emailová adresa zřízená Útvarem pro ochranu osobních údajů, právní záležitosti a oblast compliance nebo určena kontaktní osoba, kterou lze přímo kontaktovat online).

(5) Pracovník příslušné společnosti odpovědný za ochranu údajů je povinen prostřednictvím příslušného kanálu neprodleně vyrozumět pracovníka odpovědného za ochranu údajů v rámci koncernu Deutsche Telekom o jakémkoli případu porušení práv na ochranu údajů.

(6) Každý subjekt údajů je oprávněn podat stížnost podle Části V těchto Pravidel, dojde-li k porušení jeho práv nebo vznikne-li mu újma.

24. Právo na dotazy a stížnosti

Každý subjekt údajů je má právo kdykoli kontaktovat pracovníka odpovědného za ochranu osobních údajů v příslušné společnosti, která používá jeho osobní údaje, s dotazy a stížnostmi v souvislosti s aplikací těchto Pravidel pro ochranu údajů. Společnost, která je nejlépe obeznámena s konkrétním případem, nebo společnost, která shromáždila údaje o daném subjektu údajů, následně zajistí, aby i ostatní odpovědné společnosti řádně zachovávaly práva dotčeného subjektu údajů.

25. Výkon práv subjektů údajů

Subjekty údajů nesmí být z důvodu využití těchto svých práv znevýhodněny. Způsob komunikace se subjektem údajů – např. telefonický, elektronický či písemný kontakt – by měl v příslušných případech brát ohled na požadavek subjektu údajů.

Písemná kopie Pravidel
Písemná kopie těchto Pravidel bude kterémukoli zájemci poskytnuta na požádání.

IV. Řízení procesu ochrany údajů

26. Odpovědnost za zpracování údajů

Jednotlivé společnosti jsou povinny zajistit dodržování zákonných ustanovení upravujících ochranu osobních údajů, jakož i ustanovení těchto Pravidel .

27. Zmocněnec odpovědný za ochranu osobních údajů

(1) Každá společnost jmenuje nezávislého zmocněnce odpovědného za ochranu osobních údajů (*Data Privacy Officer*), jehož úkolem bude zajistit, aby byly jednotlivé organizační útvary v rámci dané společnosti informovány o požadavcích na ochranu osobních údajů stanovených v právních předpisech, interních předpisech platných v rámci příslušné společnosti/koncernu Deutsche Telekom a zejména v těchto Pravidlech. Zmocněnec odpovědný za ochranu osobních údajů využije ke sledování, zda jsou ustanovení na ochranu údajů náležitě dodržována, vhodná opatření, zejména namátkové kontroly.

(2) Před jmenováním zmocněnce odpovědného za ochranu údajů projedná příslušná společnost tuto záležitost se zmocněncem odpovědným za ochranu údajů v rámci koncernu Deutsche Telekom.

(3) Každá společnost v rámci koncernu Deutsche Telekom je povinna zajistit, aby měl zmocněnec odpovědný za ochranu osobních údajů příslušné znalosti a zkušenosti, které mu umožní vyhodnocovat právní, technické a organizační aspekty opatření na ochranu osobních údajů.

(4) Příslušná společnost poskytne zmocněnci odpovědnému za ochranu údajů finanční a lidské zdroje nezbytné k výkonu jeho povinností.

(5) Zmocněnec odpovědný za ochranu osobních údajů bude přímo podřízen vedení dané společnosti a bude na vedení společnosti organizačně napojen.

(6) Zmocněnec každé společnosti odpovědný za ochranu osobních údajů ponese odpovědnost za realizaci požadavků pracovníka odpovědného za ochranu osobních údajů v rámci koncernu Deutsche Telekom a požadavků vyplývajících ze strategie koncernu Deutsche Telekom týkající se ochrany osobních údajů.

(7) Všechny útvary každé společnosti jsou povinny vyrozumět zmocněnce dané společnosti odpovědného za ochranu osobních údajů o veškerých změnách v IT infrastruktuře, síťové infrastruktuře, business modelech, produktech, zpracování zaměstnaneckých osobních údajů a odpovídajících strategických plánů. Zmocněnec odpovědný za ochranu údajů bude přizván k projednávání změn již v rané fázi, aby bylo

zajištěno zohlednění a vyhodnocení jejich dopadu na ochranu osobních údajů.

28. Zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom

(1) Proces spolupráce a zajištění shody ohledně všech významných otázek týkajících se ochrany osobních údajů v rámci koncernu Deutsche Telekom bude koordinovat zmocněnec odpovědný za ochranu údajů v rámci koncernu Deutsche Telekom (*Group Data Privacy Officer*). Tento zmocněnec bude informovat generálního ředitele holdingové společnosti koncernu Deutsche Telekom o vývoji v této oblasti a v případě potřeby bude navrhovat doporučení.

(2) Povinností zmocněnce odpovědného za ochranu osobních údajů v rámci koncernu Deutsche Telekom bude připravovat a rozpracovávat strategii koncernu Deutsche Telekom týkající se ochrany osobních údajů a v případě potřeby poskytovat poradenství pracovníkům na ochranu osobních údajů v jednotlivých společnostech v rámci koncernu Deutsche Telekom. Tito pracovníci pak rozpracují strategii ochrany osobních údajů pro své společnosti v souladu se strategií ochrany osobních údajů platnou pro celý koncern. Zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom spolu s pracovníky odpovědnými za ochranu osobních údajů v jednotlivých provozních společnostech se budou každoročně scházet na mezinárodních jednáních o ochraně osobních údajů (*International Privacy Leader Meetings*), kde budou vzájemně sdílet získané informace.

29. Informační povinnost v případě porušení

Příslušná společnost je povinna neprodleně vyrozumět svého zmocněnce odpovědného za ochranu údajů o jakémkoli porušení či podezření na porušení předpisů upravujících ochranu osobních údajů, zejména těchto Pravidel pro ochranu údajů. V případě, že by takový incident mohl mít dopad na veřejnost, že se týká více než jedné společnosti nebo může vést k újmě vyšší než 500.00,00 eur, je zmocněnec odpovědný za ochranu osobních údajů povinen následně neprodleně vyrozumět zmocněnce odpovědného za ochranu osobních údajů v rámci koncernu Deutsche Telekom. Zmocněnec odpovědný za ochranu osobních údajů je rovněž povinen vyrozumět zmocněnce odpovědného za ochranu osobních údajů v rámci koncernu Deutsche Telekom v případě změn právních předpisů, jež je daná společnost povinna dodržovat a které významným způsobem nepříznivě ovlivňují dodržování těchto Pravidel.

30. Kontrola úrovně ochrany osobních údajů

(1) Kontroly dodržování požadavků stanovených v těchto Pravidlech a úrovně ochrany osobních údajů z něho vyplývající bude provádět zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom na základě ročního plánu kontrol i prostřednictvím jiných opatření, např. na základě auditu prováděného pracovníky odpovědnými za ochranu osobních údajů v rámci jednotlivých společností i na základě poskytovaných zpráv.

(2) Audity nařízené zmocněncem odpovědným za ochranu osobních údajů v rámci koncernu Deutsche Telekom budou provádět interní a externí auditoři. V rámci koncernu Deutsche Telekom budou rovněž prováděny pravidelné kontroly na bázi sebehodnocení, které bude koordinovat zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom. O výsledcích klíčových auditů a plnění následných opatření bude informován generální ředitel holdingové společnosti koncernu Deutsche Telekom. Na žádost bude zaslána kopie výsledků auditu i příslušnému orgánu pro dozor nad ochranou osobních údajů. Provedení auditu může rovněž iniciovat i orgán dozoru, který je příslušný ve vztahu k dané společnosti. Příslušná společnost je povinna poskytnout v rámci takového auditu maximální součinnost a následně realizovat opatření, která budou na základě auditu přijata.

(3) Příslušná společnost je povinna přijmout vhodná opatření k odstranění veškerých nedostatků zjištěných v rámci auditu a na realizaci těchto opatření bude dohlížet zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom. Pokud příslušná společnost daná opatření bez náležitého opodstatnění nezrealizuje, provede zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom vyhodnocení dopadu na ochranu osobních údajů a učiní nezbytné kroky, v případě potřeby přistoupí i k eskalaci dané záležitosti.

(4) Audity na základě příslušných plánů auditů mohou provádět i zmocněnci odpovědní za ochranu osobních údajů v jednotlivých společnostech nebo jiné organizační útvary tímto úkolem pověřené s tím, že jsou povinni písemně zdokumentovat, zda dané společnosti dodržují požadavky týkající se ochrany osobních údajů.

(5) Nebudou-li pro to existovat právní překážky, je zmocněnec odpovědný za ochranu osobních údajů

v rámci koncernu Deutsche Telekom oprávněn kontrolovat řádné nakládání s osobními údaji ve všech společnostech (resp. zmocněnci odpovědní za ochranu osobních údajů v jednotlivých společnostech jsou oprávněni tak činit v příslušné společnosti). Příslušné společnosti jsou povinny umožnit zmocněnci odpovědnému za ochranu osobních údajů v rámci koncernu Deutsche Telekom (resp. zmocněncům odpovědným za ochranu osobních údajů v jednotlivých společnostech) plný přístup k informacím potřebným k přezkoumání a vyhodnocení situace. Zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom i zmocněnci odpovědní za ochranu osobních údajů v jednotlivých společnostech jsou oprávněni v této souvislosti vydávat příslušné pokyny.

(6) V rámci prováděných auditů budou zmocněnci odpovědní za ochranu osobních údajů pokud možno uplatňovat jednotné postupy platné pro celý koncern, např. společné audity ochrany osobních údajů. Informace o těchto postupech může poskytnout zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom.

31. Zavázání a proškolení zaměstnanců

(1) Společnosti jsou povinny zavázat své zaměstnance k ochraně osobních údajů a zachovávání důvěrnosti komunikací nejpozději ke vzniku jejich pracovního poměru. V souvislosti s tímto závazkem musí být zaměstnanci dostatečně proškoleni ve znalosti předpisů na ochranu osobních údajů. Za tímto účelem zavede daná společnost vhodné postupy a vyhradí příslušné zdroje.

(2) Zaměstnanci budou pravidelně proškolováni ve znalosti základních požadavků na ochranu osobních údajů, nejméně však jednou za dva roky. Společnosti za účelem proškolování svých zaměstnanců mohou vyvinout a organizovat příslušná školení. Zmocněnec příslušné společnosti odpovědný za ochranu osobních údajů je povinen zdokumentovat absolvování těchto školení a pravidelně (na roční bázi) informovat zmocněnce odpovědného za ochranu osobních údajů v rámci koncernu Deutsche Telekom.

(3) Zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom může centrálně zajistit zdroje a procesy potřebné k příslušnému zavázání a proškolení zaměstnanců koncernu Deutsche Telekom.

32. Spolupráce s příslušnými orgány dozoru

(1) Společnosti se zavazují, že budou spolupracovat s orgánem dozoru, který je příslušný ve vztahu k dané společnosti nebo k odesilateli údajů, na základě vzájemné důvěry a že budou zejména odpovídat na jeho dotazy a řídit se jeho doporučeními.

(2) V případě změny právních předpisů vztahujících se na společnost, která by mohla mít podstatný negativní vliv na záruky poskytované těmito Pravidly, je daná společnost povinna informovat o takové změně příslušný orgán dozoru.

33. Osoby odpovědné za vyřizování dotazů

Osobami odpovědnými za vyřizování dotazů týkajících se těchto Pravidel jsou zmocněnci jednotlivých společností odpovědní za ochranu osobních údajů nebo zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom. Zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom poskytne na žádost kontaktní údaje na zmocněnce jednotlivých společností odpovědné za ochranu osobních údajů.

Zmocněnce odpovědného za ochranu osobních údajů v rámci koncernu Deutsche Telekom Kontaktní lze kontaktovat na níže uvedených adresách a telefonním čísle

datenschutz@telekom.de
privacy@telekom.de
+49-228-181-82001

během běžné pracovní doby (SEČ).

V. ODPOVĚDNOST

34. Rozsah platnosti pravidel upravujících odpovědnost

(1) Tato Část V Pravidel se uplatní výhradně na zpracování osobních údajů shromažďovaných v Evropské unii / Evropském hospodářském prostoru, které spadá do působnosti Směrnice 94/46/ES o ochraně údajů.

(2) V rámci Evropské unie / Evropského hospodářského prostoru platí ustanovení o právní odpovědnosti upravená v právních předpisech státu, v němž má daná společnost sídlo. Ve vztahu k údajům, na které se nevztahuje čl. 35 odst. 1 těchto Pravidel, se uplatní ustanovení o právní odpovědnosti upravená v právních předpisech státu, v němž má sídlo společnost, která údaje

shromáždila, nebo pokud není tato oblast právně upravena, uplatní se podmínky přijaté příslušnou společností, která údaje shromáždila.

(3) V případě, že je společnost povinna vyplatit subjektu údajů náhradu, která převyšuje samotnou újmu, vylučuje se tímto výslovně poskytnutí exemplární náhrady újmy.

35. Poskytovatel náhrady

(1) Jakákoli fyzická osoba, která utrpěla újmu v důsledku porušení jedné či více povinností vymezených v Pravidlech ze strany společnosti v rámci koncernu Deutsche Telekom nebo příjemců dat, jimž určitá společnost v rámci koncernu Deutsche Telekom údaje předala, je oprávněna uplatnit vůči dané společnosti v rámci koncernu Deutsche Telekom nárok na příslušnou náhradu újmy.

(2) Subjekt údajů je rovněž oprávněn uplatnit nárok na náhradu újmy vůči holdingové společnosti koncernu Deutsche Telekom. Pokud náhradu újmy vyplatí holdingová společnost, je tato oprávněna požadovat náhradu od společností, které za újmu nesou odpovědnost nebo které pověřily třetí stranu, která tuto újmu způsobila.

(3) Subjekt údajů je povinen uplatnit nárok na náhradu újmy nejprve vůči společnosti, která údaje předala třetí straně. V případě, že odesilatel údajů odpovědnost *de juro* či *de facto* nenese, je subjekt údajů oprávněn nárok na náhradu újmy uplatnit u společnosti, která byla příjemcem údajů. Příjemce údajů není oprávněn se v případě porušení své odpovědnosti zprostit odkazem na odpovědnost dodavatele.

(4) Subjekt údajů je oprávněn kdykoli podat stížnost u příslušného orgánu dozoru nebo u orgánu dozoru, který je příslušný ve vztahu k holdingové společnosti koncernu Deutsche Telekom.

36. Důkazní břemeno

Důkazní břemeno k prokázání řádného nakládání s osobními údaji subjektu údajů nesou příslušné společnosti.

37. Subjekt údajů jako dotčená osoba

Nenáleží-li subjektu údajů přímé právo, je oprávněn uplatnit nárok vůči společnostem, které se dopustily porušení svých smluvních povinností, jako dotčená osoba – třetí strana s odkazem na ustanovení těchto Pravidel.

38. Jurisdikce

Dle vlastního uvážení může fyzická osoba uplatnit nárok z odpovědnosti v jurisdikci

a) které podléhá daná fyzická osoba; nebo

b) které podléhá společnost v rámci koncernu, která údaje dále předala jako první; nebo

c) podle ústředí v Evropské unii nebo sídla jednotlivé společnosti ve státě, který je členem Evropské unie, a to na základě delegované odpovědnosti za ochranu údajů.

39. Mimosoudní rozhodčí řízení

(1) Třetí strany, které mají za to, že v důsledku skutečného či domnělého použití jejich osobních údajů došlo k porušení jejich práv na ochranu osobních údajů, jsou oprávněny požádat zmocněnce příslušné společnosti odpovědného za ochranu osobních údajů, aby v této záležitosti rozhodl. Zmocněnec odpovědný za ochranu osobních údajů je oprávněn stížnost přezkoumat a poučit subjekt údajů o jeho právech. Zmocněnec odpovědný za ochranu osobních údajů však při tom musí zachovat mlčenlivost o jiných osobních údajích stěžovatele, ledaže stěžovatel pracovníka odpovědného za ochranu osobních údajů této povinnosti zprostil. Na žádost dotčené osoby se strany pokusí za součinnosti subjektu údajů a zmocněnce odpovědného za ochranu osobních údajů dosáhnout smírného řešení stížnosti. Smírné řešení může rovněž zahrnovat doporučení ohledně náhrady za újmu vzniklou v důsledku porušení práv subjektu údajů na ochranu údajů. Takové doporučení bude pro příslušné společnosti závazné, pokud jimi bude vzájemně schváleno.

(2) Právo podat stížnost u příslušného orgánu dozoru nebo právo podat žalobu tím zůstává nedotčeno.

VI. ZÁVĚREČNÁ USTANOVENÍ

40. Revize a úpravy těchto Pravidel

(1) Zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom je povinen pravidelně, nejméně však jednou ročně, provádět revize Pravidel s cílem zjistit, zda jsou v souladu s příslušnými právními předpisy, a v případě potřeby provádět jejich úpravy.

(2) Veškeré významné úpravy těchto Pravidel, které je nutné provést například z důvodu, aby byl v souladu s požadavky právních předpisů, musí být odsouhlaseny s příslušným orgánem dozoru.

Takové úpravy pak budou po uplynutí příslušného přechodného období přímo platit pro všechny společnosti, které tato Pravidla podepsaly.

(3) Zmocněnec odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom je povinen vyrozumět o obsahu úpravy všechny společnosti, které přijaly tato Pravidla.

(4) Zmocněnci jednotlivých společností odpovědní za ochranu osobních údajů jsou povinni přezkoumat, zda mají úpravy těchto Pravidel důsledky pro dodržování právních předpisů v jejich zemi nebo zda jsou s nimi v rozporu. Nebude-li pro určitou společnost možné takové změny z důvodu závazných ustanovení právních předpisů implementovat, vyrozumí o tom neprodleně zmocněnce odpovědného za ochranu osobních údajů v rámci koncernu Deutsche Telekom a příslušný orgán dozoru, a bude-li to nutné, bude platnost těchto Pravidel pro ochranu údajů dočasně pozastavena.

41. Seznam kontaktních osob a společností

Pracovník odpovědný za ochranu osobních údajů v rámci koncernu Deutsche Telekom je povinen vést seznam společností, které tato Pravidla přijaly, společně se seznamem kontaktních osob v rámci těchto společností. Bude tento seznam pravidelně aktualizovat a na žádost bude informovat subjekty údajů a příslušný úřad pro ochranu údajů.

42. Procesní právo / oddělitelnost

Tato Pravidla se v případě sporů řídí procesním právem Spolkové republiky Německo.

V případě, že jednotlivá ustanovení těchto Pravidel budou nebo se stanou neplatnými, bude se mít za to, že byly nahrazeny ustanoveními, jejichž účel co nejvíce odpovídá původnímu účelu těchto Pravidel a jeho neplatných ustanovení. Pro zamezení jakýchkoli pochybností se v takových případech nebo v případě neexistence relevantních ustanovení uplatní příslušné předpisy Evropské unie na ochranu údajů.

43. Zveřejnění

Jednotlivé společnosti jsou povinny zveřejnit informace o právech subjektů údajů a ustanovení o právech dotčené osoby vhodným způsobem, např. ve formě upozornění o ochraně osobních údajů na internetu. Tyto informace musí být zveřejněny ihned, jakmile se tato Pravidla pro ochranu osobních údajů stanou pro danou společnost závazným.

VII. DEFINICE POJMŮ

Využití pseudonymů

Znamená náhradu jména dané osoby a dalších identifikačních znaků jinými charakteristikami s cílem zabránit identifikaci subjektu údajů nebo jeho identifikaci podstatně ztížit.

Anonymizace

Znamená proces změny informací takovým způsobem, že již nelze k identifikované či identifikovatelné fyzické osobě přiřadit osobní a jiné údaje nebo tak nelze učinit bez vynaložení nepřiměřeně velkého časového úsilí, nákladů a energie.

Automatizovaná individuální rozhodnutí

Znamená rozhodnutí, jež mají pro subjekt údajů právní důsledky či na něj mají významný negativní vliv a jež jsou založena výhradně na automatizovaném zpracování údajů, jehož cílem je vyhodnocení určitých osobních aspektů subjektu údajů, např. jeho pracovní výkon, bonita, spolehlivost, chování apod.

Společnost

Znamená kteroukoli společnost, která se řídí těmito Pravidly. Pro informační účely je veden samostatný seznam těchto společností, který je pravidelně aktualizován a je na vyžádání kdykoli komukoli k dispozici k nahlédnutí.

Zpracovatel údajů

Znamená jakoukoli osobu, nikoli nutně právnickou, která zpracovává osobní údaje.

Subjekt údajů

Znamená jakoukoli fyzickou osobu, s jejímiž osobními údaji koncern Deutsche Telekom nakládá.

Koncern Deutsche Telekom

Znamená společnost Deutsche Telekom AG a veškeré společnosti, v nichž Deutsche Telekom AG přímo či nepřímo vlastní podíl přesahující 50 % či které plně ovládá.

Holdingová společnost

Znamená v současné době společnost Deutsche Telekom AG se sídlem Friedrich-Ebert-Allee 140, 53113 Bonn, Spolková republika Německo.

Osobní údaje

Znamená veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě (subjektu údajů); identifikovatelná osoba znamená osobu, kterou lze přímo či nepřímo identifikovat, zejména pak pomocí identifikačního čísla či jednoho či více faktorů specifických pro její fyzickou, fyziologickou, mentální, ekonomickou, kulturní či sociální identitu.

Příjemce

Znamená jakoukoli fyzickou či právnickou osobu, orgán státní správy či samosprávy nebo jakýkoli jiný subjekt, jemuž jsou osobní údaje zpřístupněny, ať již jde o třetí stranu či nikoli. Orgány veřejné správy, které mohou údaje případně obdržet v rámci jednotlivého dotazu, však nejsou za příjemce považovány.

Citlivé osobní údaje

Znamená údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském či filozofickém přesvědčení, členství v odborech nebo o zdraví či sexuálním životě.

Třetí strana

Znamená jinou osobu či zpracovatele údajů, než je správce údajů. Mezi třetí strany nepatří subjekty údajů ani osoby či zpracovatelé, kteří jsou pověřeni shromažďováním, zpracováváním či používáním osobních údajů ve Spolkové republice Německo, jiném členském státu Evropské unie či jiném státu, jenž uzavřel Dohodu o evropském hospodářském prostoru.

Použití

Znamená veškeré nakládání s osobními údaji, zejména shromažďování, zpracovávání a použití takových údajů, včetně jejich předávání.

Zpracování cookies

T-Mobile Czech Republic a.s. se sídlem Tomíčkova 2144/1, 148 00 Praha 4, IČ 649 49 681
zapsána do obchodního rejstříku vedeného Městským soudem v Praze, oddíl B, vložka 3787

1. Dovolujeme si vás informovat, že naše servery využívají pro svoji činnost malá množství dat, která posílají vašemu koncovému zařízení a která umožňují zejména přizpůsobení našich stránek vašim potřebám a zlepšení využití našich serverů (tzv. cookies). Cookies používá téměř každá internetová stránka na světě, obecně jde o užitečnou službu, protože zvyšuje uživatelskou přívětivost opakovaně navštívené internetové stránky (umožní vašemu počítači zapamatovat si navštívené stránky a vaše preferované nastavení jednotlivých stránek).
2. Cookies zpracovává zejména provozovatel serveru či příslušné webové stránky a provozovatelé reklamních systémů, které jsou na stránkách provozovány, a to po dobu nezbytnou k jejich využití, maximálně však po dobu 1 roku ode dne vytvoření příslušné cookie.
3. Žádná z našich cookie nesbírá a neobsahuje informace, jež mají povahu vašich osobních údajů a neumožňuje tedy jakkoliv identifikovat vaši osobu.
4. Standardní webové prohlížeče podporují správu cookies. V rámci nastavení prohlížečů můžete jednotlivé cookie ručně mazat, blokovat či zcela zakázat jejich použití, lze je také blokovat nebo povolit jen pro jednotlivé internetové stránky. Máte tedy kdykoliv možnost jednoduše a bezplatně zakázat zpracovávání cookies na našich stránkách, a to prostřednictvím nastavení vašeho webového prohlížeče. Pokud bude mít váš prohlížeč použití cookies povoleno, budeme vycházet z toho, že souhlasíte s využíváním standardních cookies ze strany našich serverů a webových stránek.
5. Níže uvádíme postup, jak vymazat cookies na nejběžněji používaných internetových prohlížečích (pro detailnější informace prosím použijte nápovědu vašeho prohlížeče):

   Internet Explorer 8 a vyšší: V nabídce „Nástroje", klikněte na „Odstranit historii prohlížení", vyberte příslušné soubory a klikněte na „Odstranit".

   Google Chrome: V nabídce „Nástroje" zvolte „Možnosti". Vyhledejte část „Ochrana osobních údajů". V části Nastavení souborů cookies klikněte na tlačítko „Zobrazit soubory cookies". Tlačítko „Odebrat vše" vymaže celý seznam souborů cookies, kliknutím na „Odebrat" vymažete Vámi vybraný, konkrétní soubor.

   Android Browser: V nabídce „Menu" klikněte na „Více", dále na „Nastavení", vyberte „Vymazat veškerá data cookies" a vymažte je kliknutím na „OK".

   Mozilla Firefox: V nabídce „Nástroje" zvolte „Možnosti" (nebo „Upravit | Předvolby" v Linuxu). V sekci „Soukromí", na panelu Cookies zvolte „Zobrazit cookies". Tlačítko „Odebrat vše" vymaže celý seznam souborů cookies, Vámi zvolené cookie odstraníte tlačítkem „Odstranit cookies".

   Safari: V nabídce zvolte „Preferences", následně „Security" a poté „Show cookies". Stisknutím tlačítka „Remove" odstraníte Opera: V nabídce „Nastavení" zvolte „Vymazat soukromá data". V Podrobných volbách vyberte „Smazat dočasné cookies" a „Smazat veškeré cookies". Cookies smažete kliknutím na „Smazat".

   Opera Mini: V nabídce „Menu" klikněte na „Nastavení". Následně klikněte na „Soukromí" a „Vymazat cookies".
6. V souvislosti s reklamními službami využívají naše stránky funkce Google Analytics v následujícím rozsahu: remarketing, přehledy zobrazení v Reklamní síti Google, integrace se službou DoubleClick Campaign Manager a demografické přehledy a přehledy zájmů. Uvedený nástroj využívá cookies zejména k optimalizaci a zobrazování reklam na základě předchozích návštěv stránek (včetně vašeho užití uvedených stránek) a k vytváření přehledů souvislostí mezi návštěvami stránek a využitím reklam či reklamních služeb a přehledů potřebných pro zájmově orientovanou inzerci. **Použití tohoto nástroje můžete omezit či zabránit v nabídce „nastavení reklam"** na adrese https://www.google.com/settings/ads.
7. V případě jakýchkoliv dotazů či připomínek nás můžete kontaktovat prostřednictvím kontaktního formuláře, který naleznete na adrese https://www.t-mobile.cz/web/cz/podpora/kontaktujte-nas.

Podmínky zpracování osobních, identifikačních, provozních a lokalizačních údajů účastníků

PODMÍNKY ZPRACOVÁNÍ OSOBNÍCH, IDENTIFIKAČNÍCH, PROVOZNÍCH A LOKALIZAČNÍCH ÚDAJŮ ÚČASTNÍKŮ SPOLEČNOSTI T-MOBILE CZECH REPUBLIC A.S. SE SÍDLEM
TOMÍČKOVA 2144/1, 148 00 PRAHA 4, IČ 649 49 681, ZAPSANÉ DO OBCHODNÍHO REJSTŘÍKU VEDENÉHO MĚSTSKÝM SOUDEM V PRAZE, ODDÍL B, VLOŽKA 3787

1. Tyto Podmínky zpracování osobních, identifikačních, provozních a lokalizačních údajů (dále jen „Podmínky") upravují práva a povinnosti smluvních stran (T-Mobile a účastníka) při zpracování osobních, identifikačních, provozních a lokalizačních údajů účastníků (dále jen „Údaje"). Za účastníka se pro účely těchto Podmínek považuje každý, kdo je s T-Mobile v jakémkoliv smluvním či obdobném vztahu. T-Mobile vede databázi, která obsahuje veškeré Údaje, které T-Mobile získal v souvislosti s uzavřením účastnické smlouvy, poskytováním nabízených služeb či jiným přímým nebo nepřímým kontaktem s účastníkem či od třetích osob. T-Mobile chrání Údaje v maximální možné míře, která odpovídá stupni technického rozvoje, a zavazuje se s nimi nakládat pouze v souladu s těmito Podmínkami a platnými právními předpisy.

2. Osobními a identifikačními údaji se rozumí zejména titul, jméno, příjmení, adresy (zejm. doručovací adresa, adresa místa instalace), rodné číslo, popř. národní identifikátor, datum narození, věk, pohlaví, vzdělání, rodinný stav, údaje o dokladech totožnosti, telefonní čísla a e-mailová spojení, obchodní firma, název, sídlo, místo podnikání, identifikační číslo, údaje o platbách a platební morálce, čísla SIM karet, účastnické telefonní číslo, aktivní tarif, heslo, provozní a lokalizační údaje a jiné údaje oprávněně získané o účastníkovi. Provozními údaji se rozumí zejména telefonní číslo volajícího, telefonní číslo volaného, druh poskytnuté služby, cena za poskytnutou službu, začátek spojení, konec spojení, datum a frekvence uskutečnění spojení, počet poskytnutých jednotek (např. minuty, kB či kusy), typ přístupu k internetu (např. WAP, APN Internet, APN Intranet, pevný internet – ADSL, SHDSL, xDSL atp.), typ používaného koncového zařízení a IMEI, konfigurační údaje (např. IP adresy), údaje o obsahu a způsobu využívání služeb a typovém chování účastníka (behaviorální údaje). Lokalizačními údaji se rozumí jakékoli údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení účastníka, zejména údaj o síti, k níž je účastník připojen (např. při roamingových spojeních), údaj o tranzitní ústředně apod. T-Mobile provádí dva základní typy zpracování Údajů: a) zpracování Údajů na základě zákona, které účastník nemůže odmítnout (viz čl. 3), a dále b) zpracování Údajů na základě zákona nebo na základě souhlasu účastníka, které účastník může kdykoliv odmítnout (viz čl. 4 a 6). T-Mobile je oprávněn Údaje zpracovávat po celou dobu trvání účastnické smlouvy, nestanoví-li tyto Podmínky či zákon pro konkrétní Údaje jinak.

3. Zpracování Údajů na základě zákona, které účastník nemůže odmítnout, zahrnuje zpracování pro následující účely: poskytování služeb, zajištění propojení a přístupu k síti, zajištění provozních činností nezbytných k poskytování služeb, vyúčtování, účetní a daňové účely, identifikace zneužívání sítě či služeb (kterým je mimo jiné i opakované neuhrazení ceny nabízených služeb), ochrany práv a právem chráněných zájmů (T-Mobile a účastníků, spočívající v posuzování schopnosti a ochoty účastníků plnit své závazky (viz čl. 5), vymáhání pohledávek z vyúčtování, poskytování služeb, prodej produktů třetích osob prostřednictvím T-Mobile či umožnění přístupu k údajům o lokalizaci, případně dalším identifikačním údajům Účastníka volajícího na čísla tísňového volání (přesný rozsah předávaných Údajů stanoví vyhláška č. 238/2007 Sb.), a to subjektům provozujícím pracoviště pro příjem volání na čísla tísňového volání.

4. Účastník souhlasí s tím, že T-Mobile je oprávněn Údaje zpracovávat k následujícím účelům: veškeré marketingové a obchodní účely (včetně zasílání obchodních sdělení, telemarketingu a provádění průzkumů trhu) společnosti T-Mobile a jakýchkoliv jiných subjektů, včetně zlepšování kvality poskytovaných služeb, poskytování služeb či služeb s přidanou hodnotou účastníkům anebo obchodním partnerům T-Mobile, ověřování způsobilosti účastníka využívat nabízené služby (zejména ověření identity a zletilosti účastníka), zveřejnění kontaktních údajů účastníka v informační službě T-Mobile, zveřejnění kontaktních údajů účastníka v informační službě jiných subjektů poskytujících tento typ služeb, zveřejnění kontaktních údajů účastníka v tištěném telefonním seznamu. V rámci zpracování Údajů pro marketingové, propagační a obchodní účely je T-Mobile oprávněn zpracovávat Údaje jak pro vlastní marketingové, propagační a obchodní aktivity, tak pro marketingové, propagační či obchodní aktivity jiných subjektů. Účastník souhlasí se zasíláním obchodních sdělení společnosti T-Mobile a jiných subjektů, přičemž obchodní sdělení je T-Mobile oprávněn zasílat elektronicky (zejména formou SMS, MMS, e-mailu) a písemně nebo je zpřístupnit v souvislosti s poskytováním kterékoli nabízené služby. Pro označení obchodních sdělení (společnosti T-Mobile i jiných subjektů) T-Mobile užívá hvězdičku (*) nebo jiné vhodné označení, které účastníka informuje o tom, že uvedené sdělení je obchodním sdělením ve smyslu platných právních předpisů a že jeho odesílatelem je T-Mobile. Účastník souhlasí s tím, že po ukončení účastnické smlouvy je T-Mobile oprávněn po dobu neurčitou zpracovávat jméno, příjmení, adresu, obchodní firmu, název, identifikační číslo a jiné kontaktní údaje účastníka (včetně telefonního čísla a e-mailové adresy), a to za účelem nabízení obchodu a služeb.

5. **T-Mobile zpracovává Údaje za účelem ověřování a hodnocení jeho bonity a platební morálky prostřednictvím registrů dlužníků či jiných podobných registrů a dále za účelem vzájemného informování oprávněných uživatelů těchto registrů, a to jak při vzniku smluvního vztahu, tak kdykoliv v průběhu trvání smlouvy, je-li to třeba.** Zpracování Údajů za účelem ověřování bonity a platební morálky a vzájemného informování oprávněných uživatelů registrů dlužníků prostřednictvím těchto registrů zahrnuje zpracování jména, příjmení, adresy, rodného čísla, názvu, obchodní firmy, sídla, místa podnikání, identifikačního čísla, data vzniku dluhu, výše dluhu, typu služby či produktu, při jejichž poskytování či prodeji dluh vznikl, splatnosti, výše dlužné částky po splatnosti, počtu dlužných vyúčtování, údajů o postoupení pohledávky, data zaplacení, údajů o odpisu pohledávky a ID záznamu. Tyto Údaje je T-Mobile oprávněn předat registru dlužníků v případě opakovaného prodlení s úhradou nebo existence jakékoliv peněžní pohledávky déle než 30 dnů po splatnosti. Provozovatel registru dlužníků je oprávněn dále tyto Údaje zpřístupnit za účelem hodnocení bonity a platební morálky všem uživatelům registru, a to včetně rodného čísla, které je nezbytným identifikátorem. K datu nabytí účinnosti těchto Podmínek T-Mobile předává data za účelem ověřování platební morálky prostřednictvím registru dlužníků sdružení SOLUS, zájmovému sdružení právnických osob, IČ 69346925. Aktuální seznam členů sdružení SOLUS je uveden na www.solus.cz. T-Mobile může rozšířit zpracování i na další registry dlužníků, v takovém případě T-Mobile pouze zveřejní na internetových stránkách.

6. **Účastník souhlasí s tím, že T-Mobile zpracovává Údaje za účelem ověřování a hodnocení jeho bonity a platební morálky prostřednictvím pozitivních registrů či jiných podobných registrů a dále za účelem vzájemného informování oprávněných uživatelů těchto registrů, a to jak při vzniku smluvního vztahu, tak kdykoliv v průběhu trvání smlouvy, je-li to třeba..** Zpracování Údajů za účelem ověřování platební morálky a vzájemného informování oprávněných uživatelů pozitivních registrů prostřednictvím těchto registrů zahrnuje zpracování jména, příjmení, adresy, rodného čísla, data narození, pohlaví, názvu, obchodní firmy, sídla, místa podnikání, identifikačního čísla, údajů o dokladech totožnosti, údajů o tom, že mezi účastníkem a T-Mobile došlo k uzavření smlouvy, údajů o finančních závazcích, které vznikly, vzniknou nebo mohou vzniknout účastníkovi vůči T-Mobile v souvislosti se smlouvou, a o plnění těchto závazků (zejm. údajů o vystavených vyúčtováních služeb), údajů o zajištění závazků účastníka souvisejících se smlouvou, dalších údajů vypovídajících o bonitě a platební morálce účastníka (zejm. údajů o rozsahu a povaze příp. porušení smluvní povinnosti, jehož následkem je existence dlužné pohledávky po splatnosti, o příp. změnách závazku nebo smlouvy, o předčasném splnění dluhu apod.). Provozovatel pozitivního registru je oprávněn dále tyto Údaje zpřístupnit za účelem hodnocení bonity a platební morálky všem uživatelům registru, a to včetně rodného čísla, které je nezbytným identifikátorem. K datu nabytí účinnosti těchto Podmínek T-Mobile předává data za účelem ověřování platební morálky prostřednictvím

pozitivního registru sdružení SOLUS, zájmovému sdružení právnických osob, IČ 69346925, . Aktuální seznam členů sdružení SOLUS je uveden na www.solus.cz. . . Souhlas ke zpracování Údajů za účelem ověřování bonity a platební morálky a za účelem vzájemného informování oprávněných uživatelů výše uvedených pozitivních registrů prostřednictvím těchto registrů dává účastník na dobu platnosti smlouvy a dále po dobu 1 roku od úhrady posledního závazku účastníka vůči T-Mobile, resp. 3 let, pokud byla účastníkova pohledávka postoupena dle platných právních předpisů. V případě pozitivního registru, pokud tato doba přesáhne dobu 10 let, budou údaje z platební historie starší 10 let zlikvidovány. T-Mobile může rozšířit zpracování i na další pozitivní registry, a to aniž by bylo nutné získat dodatečný souhlas účastníka. V takovém případě T-Mobile pouze zveřejní na internetových stránkách www.t-mobile.cz a prostřednictvím SMS zprávy informaci o přistoupení k pozitivnímu registru.

7. T-Mobile zveřejní kontaktní údaje účastníka (jméno, příjmení, adresu trvalého pobytu, případně obchodní firmu/název, adresu sídla/místa podnikání; telefonní čísla a adresu elektronické pošty, případně další dohodnuté údaje) ve vlastní informační službě, v informační službě jiných provozovatelů či v tištěném telefonním seznamu pouze v případě, že k tomu dá účastník souhlas při uzavírání účastnické smlouvy či později se jinak jednoznačně vyjádří, že k některé z uvedených aktivit dává svůj souhlas. Účelem takového zpracování kontaktních údajů je umožnit vyhledávání podrobného kontaktu o účastníkovi na základě jeho jména nebo případně nezbytného minimálního množství dalších identifikačních prvků. Opravu tištěného telefonního seznamu lze provést pouze při jeho nejbližší redakci. Účastník je oprávněn požádat, aby bylo u jeho Údajů v tištěném telefonním seznamu uvedeno, že si nepřeje být kontaktován za účelem nabízení obchodu a služeb.

8. Účastník souhlasí s tím, že jeho rozhovor se zaměstnanci T-Mobile při osobním projednávání jeho stížnosti či podnětu v prostorách osobní péče T-Mobile může být zachycen formou zvukového záznamu, a to za účelem zajištění důkazu o průběhu komunikace mezi účastníkem a zaměstnanci T-Mobile. Účastník dále souhlasí s tím, že jeho telefonní hovor s informačními službami a Zákaznickým centrem T-Mobile či externími operátorskými centry T-Mobile může být nahráván, a to za účelem vnitřní kontroly služeb a zvyšování jejich kvality či za účelem zajištění důkazu o transakci uskutečněné prostřednictvím informačních služeb, Zákaznického centra či externího operátorského centra T-Mobile.

9. Zpracování Údajů dle čl. 4, 6 a 7je účastník oprávněn kdykoliv odmítnout, resp. je oprávněn odvolat souhlas, a to buď písemně dopisem zaslaným na adresu Úseku služeb zákazníkům, telefonicky zavoláním do Zákaznického centra (800 73 73 73) či jiným způsobem stanoveným T-Mobile. V případě obchodních sdělení zasílaných formou SMS či MMS je účastník oprávněn kontaktovat T-Mobile prostřednictvím telefonního čísla, ze kterého mu bylo obchodní sdělení doručeno. Jestliže účastník odvolá svůj souhlas s určitým zpracováním Údajů, T-Mobile zpracování ukončí v přiměřené lhůtě, která odpovídá technickým a administrativním možnostem T-Mobile.

10. Účastník má právo na přístup k osobním údajům týkajícím se jeho osoby, právo na opravu těchto osobních údajů (zejména jsou-li chybné nebo neúplné), jakož i právo žádat (a to v souladu s § 21 zákona č. 101/2000 Sb., o ochraně osobních údajů, v platném znění) u společnosti T-Mobile vysvětlení a odstranění nežádoucího stavu, především má-li za to, že jsou jeho osobní údaje zpracovávány v rozporu s ochranou jeho soukromého a osobního života nebo v rozporu se zákonem.

11. Detailní informace o zpracování Údajů jsou zveřejněny na internetových stránkách www.tmobile.cz. Na těchto stránkách lze nalézt například seznam zpracovatelů osobních údajů, kteří mohou zpracovávat osobní údaje účastníků, a to na základě smlouvy o zpracování osobních údajů uzavřené mezi T-Mobile a zpracovatelem v souladu s § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů, v platném znění.

12. Tyto Podmínky nabývají platnosti a účinnosti dne 30. dubna 2016