

OBSAH

Abstrakt a klíčová slova / Abstract and Keywords.....	9
Poděkování.....	11
Seznam nejvýznamnějších pojmů.....	13
Seznam užitých zkratk.....	17
1 Úvod.....	19
1.1 Zaměření monografie.....	21
1.2 Odůvodnění užití pluralitní terminologie.....	23
1.3 Cíl monografie a dílčí otázky.....	25
1.4 Struktura monografie.....	30
1.5 Metodologie.....	31
2 Riziko a důsledky neoprávněného přístupu k osobním údajům v digitalizované společnosti.....	35
2.1 Porušení bezpečnosti osobních údajů jako bezpečnostní incident.....	35
2.2 Podoby, rozsah a trend.....	38
2.3 Újma hrozící v důsledku porušení bezpečnosti osobních údajů.....	42
2.4 Shrnutí kapitoly.....	46
3 Právní úprava povinností spojených s porušením bezpečnosti.....	49
3.1 Povinnosti před použitelností Obecného nařízení.....	50
3.1.1 Poskytovatelé veřejně dostupných služeb elektronických komunikací.....	51
3.1.2 Národní úpravy povinností ve spojitosti s porušením bezpečnosti.....	55
3.2 Ohlašování, oznamování a dokumentace porušení zabezpečení dle Obecného nařízení.....	56
3.2.1 Legislativní vývoj relevantních ustanovení Obecného nařízení.....	56
3.2.2 Struktura normativní úpravy a její složky.....	63
3.2.3 Diskuse právní úpravy povinností dle článků 33 a 34 Obecného nařízení.....	79

3.3	Povinnosti při porušení bezpečnosti v právu Spojených států amerických	92
3.3.1	Terminologie problematiky v kontextu práva Spojených států amerických	94
3.3.2	Relevantní specifika americké právní úpravy	94
3.3.3	Struktura úpravy v právu států Spojených států amerických	97
3.3.4	Judikatura a činnost státních Attorney General ve vztahu k porušením bezpečnosti	105
3.3.5	Federální úprava	108
3.4	Diskuse přínosu americké perspektivy pro tuto monografii	113
3.5	Shrnutí kapitoly	119
4	Porušení bezpečnosti osobních údajů v kontextu internetu věcí	123
4.1	Pojem internetu věcí	126
4.2	Nové formy a vzorce zpracování osobních údajů v kontextu internetu věcí	128
4.3	Problematika zajištění bezpečnosti osobních údajů v kontextu internetu věcí	135
4.4	Specifika porušení bezpečnosti v kontextu internetu věcí	138
4.4.1	Automatizovaná komunikace mezi stroji a prostředím autonomních zařízení	140
4.4.2	Přímé a nepřímé provázanosti sítí chytrého města	146
4.4.3	Prostředí podnikových sítí a specifická situace mikropodniků	154
4.5	Výzvy pro povinnosti spojené s porušením bezpečnosti v kontextu internetu věcí	164
4.5.1	Zvýšení frekvence a množství případů porušení bezpečnosti	166
4.5.2	Zvýšení závažnosti újmy v důsledku porušení bezpečnosti	166
4.5.3	Znesnadnění odhalení porušení bezpečnosti osobních údajů	167
4.5.4	Nárůst složitosti a četnosti situací se společnými správci	168
4.6	Diskuse	169
4.7	Shrnutí kapitoly	170
5	Modelování motivace povinných subjektů pro dodržování povinností	175
5.1	Riziko a hodnocení rizika	177
5.2	Teorie rozhodování	180

5.3	Investice do kyberbezpečnosti a přínosy sdílení informací	185
5.4	Rozhodování podniku o ohlašování porušení bezpečnosti	195
5.4.1	Garcíův model	195
5.4.2	Laubebo a Böbbebo model	201
5.5	Diskuse	207
5.6	Shrnutí kapitoly	211
6	Povinnosti spojené s porušením bezpečnosti osobních údajů v prostředí internetu věcí	215
6.1	Regulatorní reflexe specifík zpracování osobních údajů v prostředí internetu věcí	217
6.1.1	Provázanost regulatorních rovin dopadajících na internet věcí	218
6.1.2	Přiřazení povinností v situacích ad hoc společných správců	221
6.1.3	Koordinovaný regulatorní přístup a certifikace zařízení internetu věcí	223
6.2	Uspřádání výkladu a plnění příslušných povinností	226
6.2.1	Pokyny, doporučení a osvědčené postupy	226
6.2.2	Kodexy chování a standardizace	227
6.2.3	Vydávání osvědčení a zavedení pečeti a známek	230
6.3	Podpora sdílení informací pro zvýšení kooperace a synergií mezi podniky	231
6.3.1	Centra pro analýzu a sdílení informací	232
6.3.2	Iniciativy směřující ke sdílení informací v rámci EU	233
6.3.3	Překážky sdílení informací	235
6.4	Posílení přenositelnosti vzniklé újmy zpět na odpovědné subjekty	236
6.4.1	Nárok na náhradu újmy dle Obecného nařízení	236
6.4.2	Právní rámce pro skupinové žaloby v EU	237
6.4.3	Právní úprava zástupných žalob	239
6.5	Účelné propojení s hlášením kybernetických bezpečnostních incidentů	242
6.5.1	Hlášení kybernetických bezpečnostních incidentů	243
6.5.2	Rostoucí obsahový překryv v prostředí internetu věcí	248
6.5.3	Přínosy systematické institucionální spolupráce	252

6.6	Uspodnění odhalení neohlášených případů porušení zabezpečení.....	254
6.6.1	Zavedené postupy pro odhalování zranitelností.....	255
6.6.2	Ochrana oznamovatelů porušení unijního práva.....	256
6.6.3	Přínosy a překážky využití motivačních nástrojů.....	258
6.7	Shrnutí kapitoly.....	259
7	Závěr.....	265
	Summary – Personal Data Breach in the Context of the Internet of Things.....	275
	Literatura a další použité zdroje.....	283
	Právní předpisy.....	283
	Národní právní předpisy.....	283
	Primární právo EU.....	283
	Sekundární právo EU.....	283
	Americké právní předpisy.....	286
	Ostatní právní předpisy.....	288
	Judikatura.....	288
	Soudní dvůr Evropské unie.....	288
	Nejvyšší soud Spojených států amerických.....	288
	Další americké soudy.....	289
	Monografie, odborné články, sborníky a další online zdroje.....	289