

OBSAH

Seznam zkratk	17
Kapitola 1 Úvod	21
1.1 Co by měla tato publikace přinést	21
1.2 Proč je důležité chránit osobní údaje	22
1.3 Důvody pro přijetí změny legislativy Evropské unie i České republiky.....	23
1.4 Ochrana osobních údajů od minulosti do současnosti – krátký historický exkurz	25
1.4.1 Vývoj ochrany osobních údajů ve světě a v Evropě	26
1.4.2 Vývoj ochrany osobních údajů na území České republiky	28
1.5 Stručná charakteristika nové právní úpravy založené na GDPR a toho, co přináší	28
1.5.1 Obecný přínos	28
1.5.2 Proč je GDPR nařízení a nikoli směrnice	29
1.5.3 Cíle GDPR.....	30
1.5.4 Platnost a účinnost GDPR	31
1.5.5 GDPR a české zákony	31
1.5.6 Dva nové přístupy	32
1.5.6.1 <i>Princip odpovědnosti správce</i>	32
1.5.6.2 <i>Přístup založený na riziku</i>	32
1.5.7 Nové povinnosti podle GDPR.....	33
Kapitola 2 Objasnění systému právních předpisů z oblasti ochrany osobních údajů v kontextu EU a definice klíčových pojmů z oblasti GDPR	34
2.1 Systém právních předpisů z oblasti ochrany osobních údajů v kontextu EU	34
2.2 Základní zásady pro zpracování osobních údajů	38
2.3 Definice klíčových pojmů.....	44
Kapitola 3 Ochrana osob v případě porušení osobnostních práv nebo ochrany osobních údajů	53
3.1 Ochrana osob v případě porušení osobnostních práv.....	53
3.2 Neoprávněný zásah.....	53

3.2.1	Nároky z porušení nebo ohrožení osobnostních práv	54
3.2.1.1	Nárok na zdržení se zásahů.....	55
3.2.1.2	Nárok na odstranění následků neoprávněného zásahu	56
3.2.1.3	Nárok na náhradu újmy.....	56
3.2.2	Ochrana práva na jméno.....	58
3.2.3	Ochrana pseudonymu	59
3.2.4	Ochrana práva na podobu a k podobizně.....	59
3.3	Ochrana osobních údajů	59
3.3.1	Obecně k ochraně osobních údajů v GDPR.....	59
3.3.2	Stížnost u dozorového úřadu (u nás Úřadu pro ochranu osobních údajů)	59
3.3.3	Soudní přezkum činnosti dozorového orgánu.....	60
3.3.4	Soudní ochrana v případě nečinnosti dozorového orgánu	61
3.3.5	Soudní ochrana v případě porušení práv zpracovatelem nebo správcem.....	61
Kapitola 4 Shrnutí povinností podle legislativního stavu před nabytím účinnosti GDPR.....		63
4.1	Hlavní zásady	63
4.2	Oznamovací povinnost.....	63
4.3	Zpracování a dokumentování přijatých a provedených patření	64
Kapitola 5 Nová praxe aneb co přináší GDPR a předpisy s ním souvisící.....		65
5.1	Jaké nové povinnosti GDPR přináší.....	65
5.2	Jaké povinnosti GDPR mění	65
5.3	Podpora přeshraničního pohybu zboží a služeb jako jeden z aspektů GDPR.....	66
5.4	Ne všechno, co GDPR přináší, je nové.....	66
5.5	GDPR a česká legislativa.....	67
5.6	Na co se GDPR nevztahuje.....	67
5.7	Správce nebo zpracovatel mimo Evropskou unii	68
5.8	Pseudonymizované osobní údaje.....	69
5.9	Cookies a další identifikátory.....	69
5.10	Shromažďování osobních údajů pro vědecké účely	70
5.11	Hlavní provozovna z hlediska GDPR	70

5.12	Ochrana dětí.....	71
5.13	Základní pravidla zpracování osobních údajů.....	71
5.13.1	Zpracování osobních údajů se souhlasem subjektu údajů	72
5.13.2	Zpracování osobních údajů bez souhlasu subjektu údajů	72
5.14	Fotografie fyzických osob	73
5.15	Zpracování citlivých osobních údajů	73
5.16	Komunikace se subjekty údajů.....	74
5.16.1	Informace o zpracování osobních údajů.....	74
5.17	Zpracování osobních údajů pro jiný účel, než je účel, pro který byly shromážděny	75
5.18	Právo na opravu osobních údajů a právo být zapomenut	75
5.19	Předávání osobních údajů jinému správci.....	76
5.20	Námítky proti zpracování.....	76
5.21	Povinnost doložit oprávněnost zpracování osobních údajů	77
5.22	Obecná opatření pro zvýšení ochrany osobních údajů	78
5.23	Správce nebo zpracovatel, který není usazen v Evropské unii	79
5.24	Vztah správce a zpracovatele.....	79
5.25	Povinnost ohlašovat porušení zabezpečení osobních údajů.....	80
5.26	Posouzení vlivu na ochranu osobních údajů	81
5.27	Role podnikatelských sdružení.....	83
5.28	Osvědčení a certifikáty.....	83
5.29	Předávání osobních údajů mezinárodním organizacím a do třetích zemí	84
5.30	Předávání osobních údajů, které není opakované	86
5.31	Dozorové úřady.....	87
5.32	Sbor.....	88
5.33	Stížnosti.....	89
5.34	Odčinění újmy při porušení ochrany osobních údajů.....	90
5.35	Ukládání sankcí	91
5.36	Ochrana osobních údajů v rámci novinářského, akademického, uměleckého nebo literárního projevu.....	92
5.37	Ochrana osobních údajů a veřejný přístup k informacím.....	92
5.38	Ochrana osobních údajů v pracovněprávních vztazích.....	93
5.39	Ochrana osobních údajů pro účely archivace ve veřejném zájmu ..	93
5.40	Ochrana osobních údajů ve vědeckém výzkumu	94
5.41	Ochrana osobních údajů ve statistice.....	95
5.42	Ochrana osobních údajů v rámci církve nebo náboženského sdružení či společenství.....	95

5.43	Nástroje proti porušování ochrany osobních údajů ve třetích zemích	95
Kapitola 6 Zavádění GDPR		97
6.1	Zavádění GDPR do činnosti podnikatelských subjektů.....	97
6.1.1	Správce a zpracovatel	97
6.1.1.1	<i>Odpovědnost správce</i>	<i>97</i>
6.1.2	Záměrná a standardní ochrana osobních údajů	97
6.1.3	Společní správci	98
6.1.4	Zástupci správců nebo zpracovatelů, kteří nejsou usazeni v Evropské unii	98
6.1.5	Zpracovatel	99
6.1.6	Zpracování z pověření správce nebo zpracovatele	100
6.1.7	Posouzení vlivu na ochranu osobních údajů.....	101
6.1.7.1	<i>Co tedy musí posouzení vlivu na ochranu osobních údajů obsahovat.....</i>	<i>103</i>
6.1.7.2	<i>Systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce.....</i>	<i>103</i>
6.1.7.3	<i>Posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů.....</i>	<i>104</i>
6.1.7.4	<i>Posouzení rizik pro práva a svobody subjektů údajů</i>	<i>104</i>
6.1.7.5	<i>Plánovaná opatření k řešení rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.....</i>	<i>105</i>
6.1.7.6	<i>Kodexy chování.....</i>	<i>106</i>
6.1.7.7	<i>Co se bude konkrétně posuzovat při posouzení vlivu na ochranu osobních údajů.....</i>	<i>107</i>
6.1.7.8	<i>Povinnosti osob</i>	<i>108</i>
6.1.7.9	<i>Technická opatření k zajištění ochrany osobních údajů.....</i>	<i>109</i>
6.1.8	Hlavní zásady zpracování osobních údajů.....	112
6.1.8.1	<i>Zpracování osobních údajů bez souhlasu subjektu údajů</i>	<i>113</i>

6.1.8.2	Zpracování osobních údajů se souhlasem subjektu údajů	114
6.1.8.3	Podmínky použitelné na souhlas dítěte v souvislosti se službami informační společnosti ...	115
6.1.9	Zpracování zvláštních kategorií osobních údajů (tzv. citlivé osobní údaje)	115
6.1.10	Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů	117
6.1.11	Zpracování, které nevyžaduje identifikaci	117
6.1.12	Právo subjektu údajů na přístup k osobním údajům	118
6.1.13	Oprava a výmaz	118
6.1.13.1	Právo na opravu	118
6.1.13.2	Právo na výmaz („právo být zapomenut“)	118
6.1.13.3	Výjimky z povinnosti výmazu	119
6.1.13.4	Právo na omezení zpracování	119
6.1.13.5	Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování	120
6.1.14	Právo na přenositelnost údajů	120
6.1.15	Právo vznést námitku a automatizované individuální rozhodování	121
6.1.15.1	Právo vznést námitku	121
6.1.16	Automatizované individuální rozhodování, včetně profilování	122
6.1.17	Omezení	122
6.1.18	Záznamy o činnostech zpracování	123
6.1.19	Předchozí konzultace	124
6.1.19.1	Předchozí konzultace jako nový prvek v ochraně osobních údajů	124
6.1.20	Reakce Úřadu pro ochranu osobních údajů na nedostatky zjištěné při předchozí konzultaci	125
6.1.20.1	Nápravné pravomoci úřadu	126
6.1.20.2	Pokuty	127
6.1.21	Povolovací a poradní činnost Úřadu pro ochranu osobních údajů	128
6.1.22	Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu	129
6.1.22.1	Lhůty	129

6.1.22.2	Obsah ohlášení.....	129
6.1.22.3	Příprava na případné porušení zabezpečení osobních údajů.....	130
6.1.22.4	Dokumentace případů porušení zabezpečení osobních údajů.....	130
6.1.23	Oznamování případů porušení zabezpečení osobních údajů subjektu údajů	131
6.2	Zavádění GDPR do činnosti státních úřadů	132
6.2.1	Tradice ochrany osobních údajů ve státních úřadech.....	132
6.2.2	Překážky snadného zavádění GDPR ve státní správě.....	133
6.2.3	Problémy se souhlasem subjektu údajů ve státní správě.....	133
6.2.4	Problémy s uplatněním veřejného zájmu.....	134
6.2.5	Rodná čísla	134
6.2.6	Co bude zřejmě třeba udělat při zavádění GDPR.....	134
6.3	Zavádění GDPR do činnosti samosprávných úřadů	136
6.3.1	Zvláštnosti práce s osobními údaji v samosprávných úřadech	136
6.3.2	Zastupitelstvo a rada obce.....	136
6.3.3	Zavádění GDPR v obcích.....	137
6.3.4	Projekt implementace	138
6.3.5	Sestavení projektového týmu.....	138
6.3.6	Stanovení projektových cílů.....	139
6.3.7	Lidské zdroje.....	139
6.3.8	Rozpočet.....	139
6.3.9	Harmonogram.....	139
6.3.10	Analýza procesů v organizaci	139
6.3.11	Revize stávajících souhlasů	140
6.3.12	Analýzy rizik.....	140
6.3.13	Právní audit.....	140
6.3.14	Analýza existujícího stavu, nutných požadavků a návrh řešení – GAP analýza.....	141
6.3.15	Záznamy o činnostech zpracování.....	142
6.3.16	Práva subjektů údajů.....	142
6.3.17	Školení	142
6.3.18	Dokumentace.....	142
6.3.19	Pověřenec pro ochranu osobních údajů v obci či jiném samosprávním subjektu.....	143
6.3.20	Posouzení dopadů ochrany údajů (DPIA)	143

6.3.21	Závěrečné doporučení pro menší samosprávné subjekty.....	144
6.4	Zavádění GDPR do činnosti neziskových organizací.....	144
6.4.1	Zvláštnosti práce s osobními údaji v neziskových organizacích	144
6.4.2	Postup při zavádění GDPR v neziskových organizacích...	145
6.4.3	Vnitřní politika ochrany osobních údajů.....	149
6.4.4	Autorizace a proškolení osob	150
6.4.5	Citlivé osobní údaje	151
6.4.6	Posouzení vlivu zpracování na ochranu osobních údajů (DPIA)	151
6.4.7	Pověřenec pro ochranu osobních údajů (DPO).....	151
6.4.8	Fundraising	152
6.4.8.1	<i>Adresáře z veřejně dostupných kontaktů</i>	<i>152</i>
6.4.8.2	<i>Nákup kontaktů od direct marketingových firem...</i>	<i>153</i>
6.4.8.3	<i>Udržování kontaktů a dalších údajů o sympatizantech a dobrovolnících</i>	<i>153</i>
6.4.8.4	<i>Využívání transparentních účtů.....</i>	<i>154</i>
6.4.8.5	<i>Propagace</i>	<i>155</i>
6.4.8.6	<i>Aplikace, weby a newsletterové systémy.....</i>	<i>155</i>
6.4.9	Sociální služby	156
6.4.10	Watchdogové organizace.....	158
6.4.11	Petiční právo	158
6.4.12	Organizace věnující se dětem	159
6.4.13	Kodexy chování	160
6.4.14	Právo na zastupování osob.....	161
6.5	Zavádění GDPR do činnosti zdravotnických zařízení	162
6.5.1	Tradice ochrany a zvláštnosti ochrany osobních údajů ve zdravotnictví	162
6.5.2	Národní kontaktní místo pro elektronické zdravotnictví.....	163
6.5.3	Překážky snadného zavádění GDPR ve zdravotnictví	163
6.5.4	Problémy se souhlasem subjektu údajů ve zdravotnictví.....	164
6.5.5	Osobní údaje ve zdravotnictví jako obchodní artikl	164
6.5.6	Co bude zřejmě třeba udělat při zavádění GDPR ve zdravotnictví.....	164
Kapitola 7 GDPR z hlediska IT a IS problematiky		165
7.1	Organizační záležitosti projektu uvedení do souladu s GDPR	165

7.1.1	Analýza současného stavu.....	166
7.1.2	Interní audit nakládání s osobními údaji a jejich ochrany.....	167
7.1.2.1	<i>Posouzení stavu informační bezpečnosti.....</i>	<i>169</i>
7.1.3	Rozdílová (GAP) analýza.....	170
7.1.4	Analýza dopadů.....	170
7.1.4.1	<i>Naplnění procesů realizujících práva na transparent- nost a přenositelnost.....</i>	<i>170</i>
7.1.4.2	<i>Naplnění práva být zapomenut.....</i>	<i>170</i>
7.1.4.3	<i>Čištění a migrace dat a souhlasů v den spuštění</i>	<i>171</i>
7.1.4.4	<i>Nastavení procesů a postupů pro budoucí provoz IT systémů</i>	<i>171</i>
7.1.4.5	<i>Posouzení vlivu na ochranu osobních údajů</i>	<i>171</i>
7.1.5	Doporučené postupy	172
7.2	Bezpečnost IT systémů a „Privacy by design a by default“ (sukromí již v návrhu)	172
7.2.1	Přístupy k bezpečnému zpracování dat.....	173
7.2.2	Pseudonymizace	174
7.2.3	Šifrování dat.....	175
7.2.4	Předávání dat třetím subjektům	175
7.2.5	Auditování.....	175
7.2.6	Síťová infrastruktura a fyzické zabezpečení.....	176
7.2.7	Aktivní předcházení úniku dat.....	176
7.2.8	Připravenost na bezpečnostní incidenty	177
7.3	Implementace nových systémů a procesů	177
7.3.1	Základní přístupy, centralizace správy dat.....	178
7.3.2	Správa souhlasů	179
7.3.3	Právo na transparentnost a přenositelnost	179
7.3.4	Právo na výmaz, právo být zapomenut	181
7.4	Příprava na GDPR audit	182
7.4.1	Co je dobré mít připravené pro audit?	183
7.5	Základní atributy centralizovaného řešení pro ukládání a zpracování osobních údajů.....	183
Kapitola 8 GDPR z hlediska řídicích procesů a jejich správného nastavení.....		185
8.1	Uvedení do problematiky	185
8.2	Stručný postup nastavení procesů řízení GDPR	187
8.2.1	Příprava projektu.....	188

8.2.1.1	<i>Cíle projektu</i>	189
8.2.1.2	<i>Aktivity přípravy projektu</i>	189
8.2.2	<i>Analýza stávajícího stavu</i>	189
8.2.2.1	<i>Vstupní interview</i>	190
8.2.2.2	<i>Sběr informací k provedení analýzy</i>	190
8.2.3	<i>Analýza rizik</i>	191
8.2.3.1	<i>Strategie a cíle</i>	192
8.2.3.2	<i>Aktiva</i>	193
8.2.3.3	<i>Rizika</i>	193
8.2.4	<i>Návrh budoucího stavu</i>	195
8.2.4.1	<i>Aktualizace strategie</i>	195
8.2.4.2	<i>Nastavení procesů (včetně procesů ochrany osobních údajů)</i>	196
8.2.4.21	<i>Základní předpoklad pro popis procesů</i>	197
8.2.5	<i>Nastavení procesů pro řízení GDPR</i>	202
8.2.5.1	<i>Strategie, cíle, rizika</i>	202
8.2.5.2	<i>Procesy z pohledu správce a zpracovatelů</i>	202
8.2.5.3	<i>Procesy práv subjektu údajů</i>	203
8.2.5.4	<i>Ostatní procesy pro GDPR</i>	203
8.3	<i>Nástroje pro podporu řízení</i>	203
8.3.1	<i>SW ARIS</i>	204
8.3.1.1	<i>Modelovací nástroje ARIS</i>	204
8.3.1.2	<i>ARIS Connect – publikace a týmová spolupráce</i>	204
8.3.2	<i>SW Risk & Compliance Manager</i>	206
Kapitola 9 GDPR z hlediska vnitřní bezpečnosti		208
9.1	<i>Bezpečnost</i>	208
9.2	<i>Technická ochrana objektu</i>	208
9.2.1	<i>Mechanické zábranné systémy</i>	210
9.3	<i>Elektronické zabezpečení</i>	216
9.3.1	<i>Poplachové zabezpečovací a tísňové systémy</i>	216
9.3.2	<i>Kamerové systémy</i>	219
9.3.3	<i>Přístupové systémy</i>	220
9.3.4	<i>Elektrická požární signalizace</i>	223
9.4	<i>Hlídací služba</i>	224
9.5	<i>Pokyny/směrnice</i>	228
Kapitola 10 GDPR z hlediska spisové služby		230
10.1	<i>Fyzické dokumenty</i>	231

10.1.1	Přijetí dokumentů a předávání dokumentů ke zpracování	232
10.1.2	Vyřizování/vytváření dokumentů/oběh dokumentů.....	232
10.1.3	Odesílání dokumentů	234
10.1.4	Ukládání dokumentů.....	234
10.1.5	Skartace	236
10.2	Elektronické dokumenty.....	237
10.3	Doporučení v oblasti spisové služby	239
Kapitola 11 Pověřenec pro ochranu osobních údajů		241
11.1	Pověřenec pro ochranu osobních údajů jako nový institut.....	241
11.2	Kdy angažovat pověřence	241
11.3	Orgány veřejné moci nebo veřejné subjekty s výjimkou soudů jednajících v rámci svých soudních pravomocí.....	242
11.3.1	Co je veřejný subjekt.....	244
11.3.2	Postavení státního podniku	246
11.4	Jmenování pověřence	248
11.5	Osoby, pokud jejich hlavní činnosti jako správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů.....	250
11.5.1	Rozsáhlé zpracování osobních údajů.....	251
11.5.2	Pravidelné a systematické monitorování.....	252
11.5.3	Kde působí pověřenec z hlediska činnosti správce a zpracovatele.....	254
11.5.4	Jmenování jediného pověřence pro více organizací	255
11.5.5	Dosažitelnost, dostupnost a sídlo pověřence pro ochranu osobních údajů.....	256
11.5.6	Komunikační schopnosti pověřence pro ochranu osobních údajů.....	258
11.5.7	Má být pověřenec pro ochranu osobních údajů zaměstnanec nebo externí pracovník	258
11.5.8	Jaké jsou výhody a nevýhody pověřenců pro ochranu osobních údajů v postavení externích odborníků u správce nebo zpracovatele	260
11.5.9	Pověřenec pro ochranu osobních údajů pro více subjektů....	261
11.5.10	Odborné znalosti a schopnosti pověřence pro ochranu osobních údajů.....	262

11.5.11	Schopnost pověřence pro ochranu osobních údajů plnit úkoly	263
11.5.12	Pověřenec pro ochranu osobních údajů pracující na základě smlouvy o poskytování služeb	264
11.5.13	Zveřejňování a sdělování kontaktních údajů pověřence	266
11.5.14	Postavení pověřence pro ochranu osobních údajů	267
11.5.15	Nezbytné zdroje.....	268
11.5.16	Pokyny a plnění povinností a úkolů nezávislým způsobem.....	270
11.5.17	Propuštění nebo sankcionování pověřence pro ochranu osobních údajů v souvislosti s plněním jeho úkolů.....	272
11.5.18	Střet zájmů	276
11.6	Úkoly pověřence pro ochranu osobních údajů.....	277
11.6.1	Monitorování souladu s GDPR.....	277
11.6.2	Role pověřence pro ochranu osobních údajů při posuzování vlivu na ochranu osobních údajů.....	278
11.6.3	Spolupráce s dozorovým úřadem a působení jako kontaktní místo	279
11.6.4	Přístup založený na riziku.....	279
11.6.5	Role pověřence pro ochranu osobních údajů při vedení záznamů.....	280

Kapitola 12 Ochrana osobnostních projevů podle občanského zákoníku

12.1	Uvedení do problematiky	283
12.2	Jednotlivé chráněné osobnostní statky	284
12.2.1	Jméno	284
12.2.2	Bydliště	288
12.2.3	Soukromí člověka.....	289
	12.2.3.1 Ochrana soukromých prostor.....	289
	12.2.3.2 Právo na informační sebeurčení	290
	12.2.3.3 Ochrana před sledováním a neoprávněným pořizováním zvukových a obrazových záznamů	292
	12.2.3.4 Ochrana soukromých písemností osobní povahy	293
12.2.4	Podoba člověka	293
12.3	Omezení práva na ochranu osobnosti	295
12.3.1	Svolení dotčené osoby	295

12.3.2	Zákonné licence.....	295
12.3.2.1	Výkon a ochrana práv.....	295
12.3.2.2	Vědecká, umělecká a zpravodajská licence, úřední účely.....	296
Kapitola 13	Jak poptávat služby v oblasti ochrany osobních údajů se zaměřením na GDPR.....	299
13.1	Zadávání služeb.....	300
13.2	Smlouvy.....	304
Kapitola 14	Doporučení pro implementaci v každodenní praxi.....	307
14.1	Návrh a jeho kvalita.....	308
14.2	Dostatek zdrojů pro změnu.....	308
14.3	Specifikace a dělba úkolů, určení odpovědných osob.....	309
14.4	Vymezení intervenční oblasti.....	309
14.5	Lidský faktor v procesu implementace návrhu.....	310
14.6	Implementace z hlediska času.....	310
14.7	Podpora připravovaných změn.....	311
14.8	Identifikace kritických faktorů a jejich možná eliminace.....	311
14.9	Realizace změn a zajištění cílů.....	312
14.10	Průběžná kontrola procesu implementace.....	312
14.11	Akce zaměřené na korekci nebo nápravu.....	312
Kapitola 15	Několik zajímavých judikátů z oblasti ochrany osobních údajů.....	316
Závěr	319
Summary	320
Literatura	324
O autorech	325
Věcný rejstřík	329