

# OBSAH

<b>Obsah</b> .....	<b>5</b>
<b>Předmluva</b> .....	<b>10</b>
<b>Informace o firmě DATABOX</b> .....	<b>11</b>
<b>Informace o autorovi</b> .....	<b>11</b>
<b>Grafické prvky</b> .....	<b>12</b>
<b>Úvod</b> .....	<b>13</b>
Definice pojmů .....	14
Postup zavedení <i>Nářízení GDPR</i> do firmy.....	18
Právní předpisy související se zpracováním osobních údajů .....	19
<b>1. Základní informace</b> .....	<b>21</b>
1.1 Nezbytné dokumenty pro soulad s <i>Nářízením GDPR</i> .....	22
1.2 Právní tituly.....	29
1.3 Práva subjektů údajů.....	31
1.3.1 Právo na přístup k osobním údajům.....	32
1.3.2 Právo na opravu .....	33
1.3.3 Právo na výmaz (“právo být zapomenut”) .....	33
1.3.4 Právo na omezení zpracování .....	34
1.3.5 Právo na přenositelnost údajů .....	35
1.3.6 Právo vznést námitku .....	36
1.3.7 Automatizované individuální rozhodování, včetně profilování.....	37
1.3.8 Právo podat stížnost u dozorového úřadu .....	39
1.3.9 Právo na účinnou soudní ochranu .....	39
1.3.10 Právo na zastupování subjektů údajů.....	40
1.3.11 Právo na náhradu újmy a odpovědnost .....	40
1.3.12 Právo odvolat souhlas .....	41
1.3.13 Oznamovací povinnost ohledně opravy, výmazu nebo omezení zpracování..	41
1.4 Vazba práv subjektů údajů na právní tituly zpracování osobních údajů .....	42
1.5 Zásady zpracování osobních údajů .....	43
1.6 Vztahy v rámci <i>Nářízení GDPR</i> .....	45
1.6.1 Subjekt údajů – správce – zpracovatel.....	45
1.6.2 Správce – zpracovatel – sub-zpracovatel.....	46
1.6.3 Správce – zpracovatel – dozorový úřad.....	47
1.6.4 Správce – příjemce.....	48
1.7 Osobní údaje.....	49
1.7.1 Příklady možných osobních údajů.....	50
1.7.2 Typy zpracování osobních údajů.....	53
1.8 Zvláštní kategorie osobních údajů .....	54
1.8.1 Příklady zvláštní kategorie osobních údajů .....	56
1.8.2 Zpracování zvláštní kategorie osobních údajů o členství v odborových organizacích v souvislosti s odváděním členských příspěvků.....	57
1.8.3 Dynamický biometrický podpis.....	58
1.9 Kontrola ve firmě .....	59

1.10	Kontrola dozorového úřadu .....	61
1.11	Sankce .....	64
1.11.1	Obecné podmínky pro ukládání správních pokut.....	65
1.11.2	Maximální výše pokut podle <i>Nářízení GDPR</i> .....	67
<b>2.</b>	<b>Podrobné informace .....</b>	<b>71</b>
2.1	Informační povinnost.....	72
2.1.1	Zásady ochrany osobních údajů .....	74
2.1.2	Informační listina o zpracování osobních údajů – údaje byly získány od subjektu údajů .....	75
2.1.3	Informační listina o zpracování osobních údajů – údaje nebyly získány od subjektu údajů .....	77
2.1.4	Rozdíly v informačních listinách podle zdroje osobních údajů.....	80
2.1.5	Informační memorandum .....	81
2.2	Souhlas.....	82
2.2.1	Výslovný souhlas.....	87
2.2.2	Konkludentní souhlas.....	88
2.2.3	Souhlas zaměstnanců.....	88
2.3	Interní a externí smlouvy.....	90
2.3.1	Interní smlouvy .....	91
2.3.2	Externí smlouvy.....	92
2.4	Oprávněný zájem a balanční test .....	93
2.5	Správce a společní správci .....	97
2.5.1	Správce .....	97
2.5.2	Společní správci .....	99
2.6	Zpracovatel a zpracovatelská smlouva .....	101
2.6.1	Náležitosti zpracovatelské smlouvy.....	102
2.7	Technická a organizační opatření.....	106
2.7.1	Technická opatření .....	108
2.7.2	Organizační opatření .....	109
2.7.3	Technická a organizační opatření uvedená v dalších právních předpisech ..	109
2.8	Záznamy o činnostech zpracování .....	111
2.8.1	Záznamy o činnostech zpracování správce .....	113
2.8.2	Záznamy o činnostech zpracování zpracovatele.....	114
2.8.3	Rozdíly v záznamech o činnostech zpracování pro správce a zpracovatele ..	115
2.9	Pověřenec pro ochranu osobních údajů .....	117
2.9.1	Pojmy hlavní činnost, rozsáhlé zpracování a pravidelné a systematické monitorování.....	121
2.9.2	Postavení pověřence pro ochranu osobních údajů.....	123
2.9.3	Úkoly pověřence .....	124
2.10	Posouzení vlivu na ochranu osobních údajů .....	127
2.10.1	Kritéria hodnocení velikosti rizika.....	131
2.10.2	Seznam druhů operací podléhajících požadavku posouzení vlivu .....	132
2.10.3	Seznam druhů operací nepodléhajících požadavku posouzení vlivu .....	132
2.10.4	Předchozí konzultace.....	133
2.11	Dozorový úřad.....	135
2.11.1	Úkoly dozorového úřadu .....	138
2.11.2	Pravomoci dozorového úřadu.....	143
2.11.3	Vzájemná pomoc dozorových úřadů.....	147
2.11.4	Společné postupy dozorových úřadů .....	149

2.11.5	Vedoucí dozorový úřad .....	153
2.11.6	Spolupráce mezi vedoucím dozorovým úřadem a dalšími dotčenými dozorovými úřady .....	156
2.11.7	Postup pro naléhavé případy .....	158
2.12	Evropský sbor pro ochranu osobních údajů .....	160
2.12.1	Úkoly sboru .....	161
2.12.2	Vydávání stanovisek sborem .....	167
2.12.3	Řešení sporů sborem .....	171
2.12.4	Předseda sboru a jeho úkoly .....	173
2.12.5	Sekretariát sboru .....	173
2.13	Ohlašování a oznamování případů porušení zabezpečení osobních údajů .....	175
2.13.1	Určení rizika.....	177
2.13.2	Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu .....	178
2.13.3	Oznamování případů porušení zabezpečení osobních údajů subjektu údajů ..	180
2.13.4	Povinnosti zpracovatele .....	182
2.13.5	Ohlašování porušení zabezpečení podle dalších právních předpisů .....	182
2.14	Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím .....	184
2.14.1	Předání založené na rozhodnutí o odpovídající ochraně .....	188
2.14.2	Předávání založené na vhodných zárukách .....	190
2.14.3	Závazná podniková pravidla .....	192
2.14.4	Výjimky pro specifické situace.....	195
2.14.5	Privacy Shield.....	196
2.14.6	Přeshraniční zpracování osobních údajů v rámci Evropské unie .....	198

### **3. Informace podle konkrétních oblastí.....200**

3.1	Informační technologie.....	201
3.1.1	Minimální opatření pro malé firmy .....	206
3.1.2	IT především ve velkých společnostech .....	207
3.1.3	Zákony pro oblast IT .....	209
3.2	Anonymizace, šifrování, pseudonymizace .....	211
3.2.1	Anonymizace .....	212
3.2.2	Šifrování.....	212
3.2.3	Pseudonymizace .....	213
3.3	E-shopy a weby.....	214
3.3.1	Praktická opatření pro e-shopy a weby .....	215
3.4	Cookies.....	219
3.4.1	Co jsou to cookies?.....	219
3.4.2	Druhy cookies.....	219
3.4.3	Cookies a <i>Nařízení GDPR</i> .....	220
3.5	Kamerové systémy .....	222
3.6	GPS sledovací zařízení .....	227
3.6.1	GPS lokátor ve vozidle .....	228
3.6.2	Mobilní zařízení .....	228
3.6.3	Nositelná zařízení.....	228
3.6.4	Zapísovače událostí .....	229
3.6.5	Příklad České pošty.....	230
3.7	Přímý marketing.....	231
3.7.1	Přímý marketing elektronicky .....	233
3.7.2	Přímý marketing poštou .....	234

3.7.3	Přehled souvislostí <i>Nařízení GDPR</i> a zákona č. 480/2004 Sb. (zákon o některých službách informační společnosti) a jejich předpokládané změny v souvislosti s nařízením ePrivacy.....	235
3.7.4	Konkrétní případy zpracování osobních údajů pro přímý marketing .....	235
3.7.5	Vyjádření Úřadu pro ochranu osobních údajů o přímém elektronickém marketingu .....	238
3.7.6	Přímý marketing a databáze Živěfirmy.cz .....	239
3.8	Účetnictví .....	240
3.8.1	Kopírování a ukládání dokladů .....	243
3.8.2	Prokazování nároku na slevy na dani, nezdanitelné části základu daně a daňového zvýhodnění .....	244
3.8.3	Archivace .....	245
3.8.4	Sdělení pro plátce daně ze závislé činnosti v souvislosti s <i>Nařízením GDPR</i> ..	251
3.8.5	Zákony pro oblast účetnictví .....	253
3.9	Personální oddělení .....	254
3.9.1	Zpracování osobních údajů před začátkem pracovního poměru.....	256
3.9.2	Zpracování osobních údajů v průběhu pracovního poměru .....	258
3.9.3	Zpracování osobních údajů po ukončení pracovního poměru.....	261
3.9.4	Další možná zpracování v rámci personálního oddělení .....	263
3.9.5	Personální agentura.....	264
3.9.6	Zákony pro personální oddělení .....	265
3.10	Pracovní prostředí .....	266
3.10.1	Zpracování osobních údajů při dohledu nad užíváním informačních a komunikačních technologií na pracovišti.....	267
3.10.2	Zpracování osobních údajů při dohledu nad užíváním informačních a komunikačních technologií mimo pracoviště .....	270
3.10.3	Další možná zpracování v rámci pracovního prostředí .....	272
3.11	Školení zaměstnanců .....	274
3.12	Fotografie.....	277
3.12.1	Pořízení a použití fotografie podle občanského zákoníku .....	278
3.12.2	Pořízení a použití fotografie podle <i>Nařízení GDPR</i> .....	279
3.12.3	Zpracování zvláštní kategorie osobních údajů z fotografií podle <i>Nařízení GDPR</i> .....	279
3.13	Procesy opt-in, double opt-in a opt-out .....	281
3.13.1	Proces opt-in .....	281
3.13.2	Proces double opt-in.....	281
3.13.3	Proces opt-out.....	282
<b>4.</b>	<b>Informace podle oborů činnosti .....</b>	<b>284</b>
4.1	Hotelnictví a restaurace .....	285
4.1.1	Stanovisko ÚOOÚ č. 7/2012 – Evidence ubytovaných osob.....	289
4.2	Reality .....	293
4.3	Zdravotnictví.....	295
4.3.1	Ambulantní sféra.....	300
4.3.2	Laboratoře.....	301
4.3.3	Zákony pro oblast zdravotnictví .....	302
4.4	Školství.....	304
4.4.1	Dotace.....	310
4.4.2	Fotografie .....	311
4.4.3	Zákony pro oblast školství.....	312

4.5	Obce .....	314
4.5.1	Mají povinnost ustanovit pověřence také organizační složky obce nebo právnícké osoby zřízené či založené obcí? .....	318
4.5.2	Zákony pro oblast obcí .....	320
<b>Přílohy A – vzorové dokumenty .....</b>		<b>322</b>
A.1	Směrnice o ochraně osobních údajů .....	323
A.2	Zásady ochrany osobních údajů pro obchodní partnery .....	325
A.3	Informační listina v případě, že osobní údaje byly získány od subjektu údajů .....	327
A.4	Souhlas se zpracováním osobních údajů .....	329
A.5	Dodatek do pracovní smlouvy .....	330
A.6	Balanční test .....	331
A.7	Smlouva pro společné správce .....	332
A.8	Zpracovatelská smlouva .....	334
A.9	Konkrétní povolení k zapojení dalšího zpracovatele .....	337
A.10	Záznamy o činnostech zpracování pro kamerový systém – správce .....	338
A.11	Smlouva mezi externím pověřencem a správcem .....	340
A.12	Ohlášení porušení zabezpečení dozorovému úřadu .....	342
A.13	Osobní dotazník pro zaměstnance .....	323
A.14	Zápis ze školení zaměstnanců .....	344
<b>Přílohy B – příklady .....</b>		<b>346</b>
B.1	Bezpečnostní opatření podle ČSN EN ISO/IEC 27001 .....	346
B.2	Porušení zabezpečení a nutnost jejich ohlášení dozorovému úřadu, případně oznámení subjektu údajů .....	350
B.3	Informace o zpracování osobních údajů na e-shopu nebo webu .....	353
B.4	Informace o používání souborů cookies .....	355
B.5	Piktogram pro kamerový systém .....	356
<b>Předpokládané rozdíly adaptačního zákona a Nařízení GDPR .....</b>		<b>357</b>
<b>Zkratky .....</b>		<b>363</b>
<b>Další užitečné zdroje informací .....</b>		<b>367</b>