

Luděk Nezmar

GDPR

PRAKTICKÝ PRŮVODCE IMPLEMENTACÍ

- bezpečnost informací
- hodnota dat
- ISO 27001 a použití v GDPR
- postupy, procesy, příklady
- úkoly a povinnosti pověřence
- identifikace zpracování



Luděk Nezmar

GDPR

PRAKTICKÝ PRŮVODCE
IMPLEMENTACÍ

Grada Publishing



Upozornění pro čtenáře a uživatele této knihy

Všechna práva vyhrazena. Žádná část této tištěné či elektronické knihy nesmí být reprodukována a šířena v papírové, elektronické či jiné podobě bez předchozího písemného souhlasu nakladatele. Neoprávněné užití této knihy bude trestně stíháno.

Edice Právo pro praxi

Ing., Mgr. Luděk Nezmar, MBA

GDPR: Praktický průvodce implementací

Vydala GRADA Publishing, a.s.
U Průhonu 22, Praha 7
tel.: 234 264 401, fax 234 264 400
www.grada.cz
jako svou 6 761. publikaci

Realizace obálky Michal Němec
Sazba Jan Šístek
Odborná redaktorka Ing. Michaela Průšová
Počet stran 304
První vydání, Praha 2017
Vytiskla tiskárna Tisk Centrum, s.r.o., Moravany

© GRADA Publishing, a.s., 2017

ISBN 978-80-271-0921-0 (ePub)
ISBN 978-80-271-0920-3 (PDF)
ISBN 978-80-271-0668-4 (print)

Obsah

1. Úvod a pozadí vzniku	13
1.1 Shrnutí	13
1.2 Pozadí vzniku GDPR	13
1.2.1 Úvod	13
1.2.2 Historie ochrany osobních dat	14
2. Hodnota osobních údajů	20
2.1 Osobní údaje a online	20
2.2 Hodnota pro firmy	23
2.3 Benefit pro spotřebitele	24
2.4 Přínosy a ztráty	25
3. Co je obecné nařízení GDPR	27
3.1 GDPR – obecné nařízení EU	27
3.1.1 Co znamená Obecné nařízení o ochraně osobních údajů?	27
3.1.2 Proč muselo dojít k revizi právního rámce ochrany osobních údajů?	27
3.1.3 S nařízením jsem nikdy nepracoval, má nějaké zvláštnosti?	28
3.1.4 Co znamená datum použitelnosti Obecného nařízení?	28
3.1.5 Co bude se současným zákonem o ochraně osobních údajů?	28
3.1.6 Kdo se bude muset Obecným nařízením řídit?	28
3.1.7 Na jaké činnosti Obecné nařízení nedopadá?	29
3.2 Nové přístupy a povinnosti	29
3.2.1 Na jakých nových přístupech je Obecné nařízení založeno?	29
3.2.2 Jak budu jako správce dokládat soulad zpracování?	29
3.2.3 Osvědčení má sloužit k prokázání souladu zpracování s nařízením.	30
3.2.4 Kdo bude vydávat kodexy a osvědčení?	30
3.2.5 Jaké nové povinnosti Obecné nařízení přináší?	30
3.2.6 Kdy musí správce provést posouzení vlivu na ochranu osobních údajů?	30
3.2.7 Kdy musí správce konzultovat zpracování dat s ÚOOÚ?	31
3.2.8 Co jsou záznamy o činnostech?	31
3.2.9 Kdo nemusí vést záznamy o činnostech zpracování?	31
3.3 Nejdůležitější pojmy	31
3.3.1 Co je zpracováním osobních údajů?	31
3.3.2 Co je osobní údaj?	31
3.3.3 Kdo je subjekt údajů?	32
3.3.4 Co se rozumí profilováním?	32
3.3.5 Kdo je správce?	32
3.3.6 Kdo je zpracovatel?	32
3.4 Zásady a právní důvody zpracování	33
3.4.1 Na jakých zásadách je Obecné nařízení postaveno?	33
3.4.2 Co se rozumí právními důvody zpracování osobních údajů?	33
3.4.3 Jaké jsou právní důvody zpracování osobních údajů subjektu údajů?	33
3.4.4 Co znamená souhlas se zpracováním osobních údajů?	34
3.4.5 Jaké jsou podmínky udělení souhlasu se zpracováním osobních údajů?	34
3.4.6 Je souhlas odvolatelný?	34

3.4.7	Jak to bude se současnými souhlasy za použitelnosti Obecného nařízení?	34
3.4.8	Mohu zpracovávat osobní údaje zveřejněné na internetu?	35
3.5	Zvláštní kategorie osobních údajů (citlivé údaje)	35
3.5.1	Proč se rozlišují zvláštní kategorie osobních údajů?	35
3.5.2	Jaké údaje spadají do zvláštní kategorie osobních údajů?	35
3.5.3	Kdy lze zvláštní kategorie osobních údajů zpracovávat?	35
3.6	Práva subjektu údajů	36
3.6.1	Jaká jsou práva subjektu údajů?	36
3.6.2	Co se rozumí přístupem k osobním údajům?	36
3.6.3	Co když jsou údaje nepřesné?	37
3.6.4	Co znamená právo být zapomenut?	37
3.6.5	Co znamená právo na přenositelnost údajů?	37
3.6.6	Kdy lze vznést námitku proti zpracování osobních údajů?	38
3.6.7	Jak rychle musí správce reagovat na podanou žádost subjektu údajů? ..	38
3.6.8	Může správce účtovat náklady v souvislosti s právy subjektu údajů? ...	38
3.6.9	Co když subjekt údajů zneužívá své právo?	39
3.7	Správce, zpracovatel	39
3.7.1	Za co správce odpovídá?	39
3.7.2	Mohou být společní správci?	39
3.7.3	Jak se mě, jako správce, dotkne Obecné nařízení?	39
3.7.4	Jak na vztah správce – zpracovatel?	39
3.7.5	Může zpracovatel zapojit do zpracování jiného zpracovatele?	40
3.8	Zabezpečení osobních údajů	40
3.8.1	Jak musí správce zabezpečit osobní údaje?	40
3.8.2	Co se rozumí porušením zabezpečení osobních údajů?	40
3.8.3	Hlášení správce při bezpečnostním incidentu ÚOOÚ	40
3.8.4	Oznámení správce při bezpečnostním incidentu subjektu údajů	41
3.8.5	Jak se určí riziko porušení zabezpečení?	41
3.8.6	Existuje povinnost správce šifrovat nebo pseudonymizovat?	41
3.9	Pověřenec pro ochranu osobních údajů	41
3.9.1	Musí mít svého pověřence každá obec?	41
3.9.2	Musí být pověřenec podřízen přímo vedení organizace?	41
3.9.3	Jaké jsou úkoly pověřence pro ochranu osobních údajů?	42
3.9.4	Jaké má mít pověřenec pro ochranu osobních údajů vzdělání?	42
3.9.5	Musí být pověřenec pro ochranu osobních údajů certifikován?	42
3.9.6	Může poskytnout pověřence i právnická osoba jako službu?	42
3.10	Předávání osobních údajů do jiných zemí	42
3.10.1	Jak lze předávat osobní údaje do zemí Evropské unie?	42
3.10.2	Jaké jsou možnosti předávání osobních údajů do zemí mimo EU?	43
3.10.3	Předání založené na rozhodnutí o odpovídající ochraně	43
3.10.4	Co se rozumí předáváním založeným na vhodných zárukách?	43
3.10.5	Co jsou závazná podniková pravidla?	43
3.11	Sankce, pokuty	43
3.11.1	Jaké jsou podmínky pro ukládání pokut?	43
3.11.2	Jak vysoká může být udělená pokuta?	44
3.11.3	Jsou při ukládání pokut polehčující či přitěžující okolnosti?	44
3.12	Různé	44
3.12.1	Platnost oznamovací povinnosti v současné podobě	44
3.12.2	Co je to skupina WP29?	44

3.12.3	Poskytuje Úřad konzultace k Obecnému nařízení?	45
3.13	Příprava na GDPR	45
3.13.1	Kontrolní seznam sebehodnocení	46
4.	Zásady a principy GDPR	49
4.1	Princip 1. – Zákonnost, korektnost a transparentnost	52
4.2	Princip 2. – Omezení účelem	54
4.2.1	Vztah mezi původním a dalšími účely	58
4.2.2	Kontext sběru údajů	59
4.2.3	Povaha údajů a dopad dalšího zpracování na subjekty údajů	59
4.3	Princip 3. – Minimalizace dat	61
4.4	Princip 4. – Přesnost	62
4.5	Princip 5. – Omezení uložení	66
4.5.1	Mazání osobních údajů v IT systémech	70
4.6	Princip 6. – Integrita a důvěrnost	74
4.6.1	Manažerská a organizační opatření	76
4.6.2	Personál	77
4.6.3	Fyzická bezpečnost	78
4.6.4	Kybernetická bezpečnost	78
4.6.5	Využití zpracovatele	80
4.6.6	Porušení zabezpečení dat	80
4.7	Princip 7. – Zodpovědný přístup a prokázání souladu	81
5.	Práva a odpovědnosti	84
5.1	Práva osob	84
5.1.1	Právo být informován	84
5.1.2	Právo na přístup	85
5.1.3	Právo na opravu	87
5.1.4	Právo na výmaz (být zapomenut)	87
5.1.5	Právo na omezení zpracování	88
5.1.6	Právo přenositelnosti	89
5.1.7	Právo vznést námitku	91
5.1.8	Práva spojená s automatizací rozhodování a profilováním	92
6.	Projekt implementace GDPR do organizace	96
6.1	GAP analýza	96
6.1.1	Výstup GAP analýzy	96
6.1.2	Postup při GAP Analýze	97
6.2	Posouzení vlivu na ochranu osobních údajů (DPIA)	98
6.2.1	Proč provádět DPIA?	99
6.2.2	Co je DPIA?	100
6.2.3	Kdy je DPIA povinné?	101
6.2.4	Kdy DPIA není vyžadováno?	105
6.2.5	DPIA u již existujících zpracování	106
6.2.6	Kdy DPIA provést?	106
6.2.7	Kdo má DPIA provést?	107
6.2.8	Metodika provádění DPIA	108
6.2.9	Zveřejnění DPIA	111
6.2.10	Doporučení k provádění DPIA	112
6.2.11	Datové toky	112

6.2.12	Příchozí data	113
6.2.13	Odchozí data	113
6.2.14	Posouzení rizik	114
6.2.15	Pseudonymizace	114
6.2.16	Riziko pro ochranu osobních údajů	116
6.2.17	Provedení posouzení vlivu na ochranu osobních údajů	116
6.2.18	Kdo se na DPIA podílí?	117
6.2.19	Zpráva o posouzení vlivu na ochranu osobních údajů	118
6.3	Rizika	121
6.3.1	Zdroje rizik	121
6.3.2	Incidenty	121
6.3.3	Hrozby	122
6.3.4	Rizika	122
6.3.5	Problémy při hodnocení rizik	123
6.3.6	Postup při hodnocení rizik	123
6.3.7	Identifikace zdrojů nebezpečí	125
6.3.8	Vyhodnocení rizik	126
6.3.9	Míra rizik	127
6.3.10	Příklady hodnocení rizik	128
7.	Souhlas se zpracováním osobních údajů	130
7.1	Souhlas	130
7.1.1	Odvolání souhlasu	131
7.1.2	Kdy není souhlas nezbytný	131
7.2	Souhlas v praxi	132
7.2.1	Pravidla pro správné získání souhlasu	133
7.3	Role souhlasu v GDPR	134
7.4	Vyžadovat souhlas vždy?	134
7.5	Zpracování osobních údajů bez souhlasu	135
7.6	Alternativy k udělení souhlasu	136
7.7	Souhlas daný svobodně	137
7.8	Konkrétní a informovaný souhlas	139
7.9	Jednoznačnost vyjádřením nebo jasnou kladnou akcí	140
7.10	Výslovný souhlas	141
7.11	Délka trvání souhlasu	141
7.12	Souhlas dítěte	142
7.13	Souhlas u zvláštní kategorie osobních dat	143
7.14	Souhlas pro účely vědeckého výzkumu	144
7.15	Kdy je souhlas neplatný?	144
7.16	Žádost o udělení souhlasu	144
7.17	Záznamy o udělených souhlasech	146
7.18	Právo odvolání souhlasu	148
7.19	Zpracování u rozsudků v trestních věcech a trestných činů	149
8.	Role a odpovědnosti v rámci GDPR	150
8.1	Odpovědnosti	150
8.1.1	Správci	150
8.1.2	Společní správci	151
8.1.3	Zpracovatelé	151
8.2	Zpracování mimo EU	153

8.2.1	Klíčové požadavky	154
8.2.2	Odpovídající ochrana	154
8.2.3	Vhodné záruky	155
8.2.4	Vymahatelnost	156
8.2.5	Závazná podniková pravidla	157
8.2.6	Omezené přenosy	157
8.3	Záznamy zpracování	158
8.4	Kontrola orgánem dohledu	159
8.5	Pověřenec pro ochranu osobních údajů	163
8.5.1	Kdo musí jmenovat pověřence pro ochranu osobních údajů?	163
8.5.2	Jmenování pověřence ochrany osobních údajů	165
8.5.3	Povinnosti pověřence ochrany osobních údajů	166
8.5.4	Působení pověřence v organizaci	168
8.5.5	Pověřenec ve vztahu k dozorovému orgánu	169
8.5.6	Pověřenec jmenovaný zpracovatelem	169
8.5.7	Snadná dosažitelnost z každého podniku	170
8.5.8	Odbornost a znalosti pověřence	171
8.5.9	Úroveň odbornosti	171
8.5.10	Profesionální kvality	171
8.5.11	Schopnost plnit své úkoly	171
8.5.12	Outsourcing pověřence	172
8.5.13	Zveřejnění a sdělování kontaktních údajů pověřence	172
8.5.14	Postavení pověřence	173
8.5.15	Úkoly pověřence	176
8.6	Hlavní činnosti	178
8.6.1	Velký rozsah	179
8.6.2	Systematické monitorování	179
8.6.3	Zvláštní kategorie údajů a údajů týkající se trestů	180
8.7	Školení	180
8.7.1	Zaměstnanci musí chápat obsah GDPR	180
8.7.2	Školení musí být relevantní	181
8.7.3	Školení musí být osobní	181
8.7.4	Zaměstnanci musí být schopni rozpoznat porušení	181
8.7.5	Kdy se školením začít	182
8.8	Personalistika	182
8.8.1	Zdravotní informace zaměstnanců	186
8.8.2	Práva zaměstnanců	187
9.	Informační technologie	189
9.1	GDPR a IT technologie	189
9.1.1	Tiskárny a reprografická technika	189
9.1.2	Zabezpečení koncových zařízení	191
9.1.3	Bezpečí přenosných zařízení	194
9.2	Kybernetická bezpečnost	195
9.2.1	Vztah GDPR a ISO norem 27001, 27018	195
9.2.2	Definice struktury	197
9.2.3	Úroveň 1 – kapitola 4 – 10 a způsob, jak lze ISMS použít pro GDPR	198
9.2.4	Úroveň 2 – procesy ISMS	201
9.2.5	Úroveň 3 – použití přílohy A 114 opatření	203

9.2.6	Úroveň 4 – úprava 114 opatření v příloze A	203
9.2.7	Úroveň 5 – opatření z jiných ISO standardů	204
9.2.8	Propojení ochrany osobních údajů s ISMS	205
9.2.9	Úprava 114 opatření	210
9.2.10	Porovnání ochrany osobních údajů a zabezpečením informací	213
9.3	Document Management System	216
9.4	Bezpečnost Wi-Fi	217
9.4.1	Pravidla bezpečné Wi-Fi	218
9.5	Heslová politika	221
9.6	Nebezpečí virů – Ransomware	228
9.7	Kameryové systémy	230
9.8	Online	232
9.8.1	Dokončování	233
9.8.2	Online zpracování	233
9.8.3	Sběr správných osobních údajů	235
9.8.4	Zachování osobních údajů	236
9.8.5	Bezpečné uchovávání osobních údajů	236
9.9	Online oznámení o ochraně osobních údajů	237
9.9.1	Zmapování zpracování informací	237
9.9.2	Sdílení dat s dalšími zpracovateli	238
9.9.3	Nad rámec právních požadavků	239
9.9.4	Nástroj pro správu nastavení osobních údajů	240
9.10	Sdílení dat	241
9.11	Šifrování	242
9.11.1	Moderní šifry	242
9.11.2	Praktické využití šifrování	243
9.11.3	Šifrování a GDPR	244
9.11.4	Šifrování v praxi	244
9.12	Dodavatelé	245
9.12.1	Kritéria pro hodnocení dodavatele	246
9.13	Cloud jako outsourcovaná služba	251
9.13.1	Technická a organizační opatření	252
9.13.2	Dokumentace	253
9.13.3	Role pověření	253
9.13.4	Subdodávky obecně	253
9.13.5	Smluvní ujednání	254
9.13.6	Certifikace a kodexy	255
9.13.7	Přenesený vztah a povinnosti správce	255
9.14	Narušení integrity dat	256
9.14.1	Hlášení	257
9.14.2	Incident není událost	258
9.14.3	Postup šetření incidentu	260
9.15	Bezpečnost „by design“	261
9.15.1	Infrastruktura	263
9.15.2	GDPR a orgány vyšetřování	267
10.	Doplňující předpisy v oblasti ochrany osobních údajů	269
10.1	Nařízení o soukromí a elektronických komunikacích (PECR)	269
10.1.1	Rozšíření působnosti nařízení	269
10.1.2	Ochrana metadat	269

10.1.3	Pravidla pro používání cookies	269
10.1.4	Ochrana proti spamu	269
10.1.5	Přímá závaznost	270
10.1.6	Podnikatelské příležitosti	270
10.2	Štít EU – USA na ochranu soukromí	270
10.2.1	Povinnosti pro členy štítu	271
10.2.2	Právo být informován	271
10.2.3	Omezení účelů použití	271
10.2.4	Povinnost minimalizace údajů	272
10.2.5	Povinnost zabezpečit údaje	272
10.2.6	Povinnost ochránit údaje předané jiné společnosti	272
10.2.7	Právo na přístup k údajům a jejich opravu	273
10.2.8	Právo podat stížnost a dosáhnout nápravy	273
10.2.9	Mechanismus ombudsmana v USA	274
11.	Mýty, fakta, otázky a odpovědi	275
11.1	Pokud chcete zpracovávat osobní údaje, musíte mít souhlas.	275
11.1.1	Odkazování na obecné nařízení jako na směrnici	276
11.1.2	Označování obecného nařízení za revoluci v právech subjektu údajů a v povinnostech správců	276
11.1.3	Rozšiřuje se definice osobního údaje	277
11.1.4	Je lepší mít paušální souhlas subjektu údajů než se zabývat jednotlivými zákonnými důvody	277
11.1.5	Šifrování je povinné	278
11.1.6	Každý, popř. téměř každý správce musí mít pověřence pro ochranu osobních údajů	278
11.1.7	Pověřenec musí mít osvědčení (certifikát)	278
11.1.8	Obecné nařízení klade na pověřence pro ochranu osobních údajů vysoké, obtížně splnitelné nároky	279
11.1.9	Správce nemůže pověřenci pro ochranu osobních údajů ukládat úkoly	279
11.1.10	Nově hrozí správcům a zpracovatelům pokuty dle obratu	279
11.2	Když se zúčastním veřejné akce, mohou organizátoři bez mého souhlasu použít mé fotografie k reklamě?	280
11.3	Na svém webu používám soubory cookie – co musím zvážit?	280
11.4	Obávám se snímku dostupného v Google Street View, co mám dělat?	281
11.5	Jaká jsou má práva týkající se mých výsledků zkoušky s tím, že je mé jméno uvedeno na vývěsce nebo nástěnce?	282
11.6	Má cestovní kancelář si vyžádala velké množství osobních údajů jako součást procesu rezervace dovolené. Jsem povinen předat tyto informace?	282
11.7	Může správce daně bez mého souhlasu získat informace o mých osobních údajích?	282
12.	Slovník pojmů ochrany osobních údajů a GDPR	283
12.1	Ochrana osobních údajů	283
12.2	General Data Protection Regulation	284
12.3	Internet a online	284

13. Vzory	287
13.1 Příklad dohody o mlčenlivosti	287
13.2 Popis pracovní pozice DPO	291
13.3 Hlášení incidentu	293
13.4 Žádost o udělení souhlasu s přímým marketingem	294
13.5 Kontrolní formulář souhlasu	295
13.6 Identifikace zpracování	296
Zdroje	300

1. Úvod a pozadí vzniku

1.1 Shrnutí

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) známé jako „GDPR“ je v platnosti a účinnost nastává 25. května 2018 po dvouleté periodě určené k přípravě. Nahrazuje tak současný zákon č. 101/2000 Sb., o ochraně osobních údajů.

V současné době lze konstatovat, že naprostá většina firem, organizací i státních institucí či samospráv „zaspala“ a tomuto nařízení nevěnovala pozornost. V této souvislosti musím upozornit na skutečnost, že se nejedná o směrnici či doporučení EU, kterou vláda musí v nějaké podobě někdy implementovat, ale jedná se o nařízení EU platné v rámci všech členských zemí bez možnosti zásadních úprav. Jinými slovy 25. května 2018 může organizace dostat pokutu v plné výši.

GDPR stanovuje firmám a organizacím mnohem větší požadavky na zabezpečení osobních dat, kontrolu procesů a výrazně zvyšuje odpovědnost pod drakonickými sankcemi až do výše 550 mil. Kč nebo 4 % z celosvětového obrátu skupiny. Počítá se vyšší sankce. Znalost, jak dodržet předpisy a prakticky aplikovat nařízení za rozumných cenových podmínek, se tak stává klíčovou kompetencí pro splnění požadavků kladených GDPR bez nadměrného finančního zatížení.

Kniha by vám měla být praktickým rádcem, jak dosáhnout souladu při zpracování osobních údajů vašich klientů, pacientů nebo zaměstnanců. Pomůže vám naplánovat a provést potřebné změny ve vašich procesech zpracování dat tak, abyste od 25. května 2018 mohli klidně usínat.

1.2 Pozadí vzniku GDPR

1.2.1 Úvod

V roce 2016 Evropská unie přijala obecné nařízení o ochraně údajů (GDPR), které je platné ve všech 28 členských státech. GDPR vstoupí v účinnost (bude vymahatelné) v květnu roku 2018. Tímto momentem bude každá organizace, instituce, obec, škola, zdravotnické zařízení nebo společnost, která ukládá nebo zpracovává osobní údaje z jakéhokoli členského státu EU, muset splnit požadavky tohoto nařízení.

Nařízení dává subjektům údajů (lidem – občanům) mnohem větší práva, stanovuje mnohem přísnější požadavky jak správcům, tak zpracovatelům (firmám a institucím) a uplatňuje výrazně vyšší sankce, než tomu bylo dosud. Společnosti budou muset zavést řadu nových postupů, aby tyto požadavky splnily. Ve stále méně stabilním ekonomickém a politickém prostředí tak všechny podniky musí reagovat vyšší rychlostí adaptace a větší mírou respektu k duševnímu vlastnictví. Základem úspěchu každé společnosti v současném digitalizovaném světě je schopnost efektivně zpracovávat informace a data, včetně jejich kvalitního zabezpečení. Nikdy předtím nebyl takový tlak na rychlost, hloubku a adopci tak zásadních změn. Organizace jsou nuceny k prudké inovaci a konkurenci. Potřeba „změny jako konstantního faktoru“ je stále přítomna – stejně jako rizika, která se mohou projevit podkopáním úspěchu. Nové předpisy vyžadují společnou a nerozdílnou odpovědnost. Znalost toho, jak dodržovat nové předpisy pomocí včasného praktického přístupu, zajistí, že dodržování předpisů nebude příliš nákladné a ve skutečnosti se použije jako nová podmínka konkurenceschopnosti.

Aby bylo možné v březnu 2018 uplatnit nařízení o obecné ochraně údajů v Evropské unii (GDPR), bude nutné, aby všichni správci a zpracovatelé údajů, kteří zpracovávají osobní údaje obyvatel EU, zavedli příslušná technická a organizační opatření. Budou muset zachovat důvěrnost, integritu, dostupnost i odolnost systémů zpracovávajících osobní data.

Staré čínské přísloví praví: „Co nemá cenu, nemá ani hodnotu.“ Také současná situace potvrzuje pravdivost tohoto rčení, protože cena informací ve světě neustále stoupá a osobní údaje se staly velmi cennou komoditou. Reálná hodnota osobních údajů se objevila teprve nedávno. Kybernetická bezpečnost je jedním z klíčových úkolů budoucnosti, protože krádež osobních údajů vystavuje občany EU významným rizikům. Současné techniky analýzy dat umožňují organizacím sledovat a předvídat individuální chování, dokážou předjímat nákupní rozhodování jedinců a mohou být nasazeny v automatizovaném rozhodování. Kombinace všech těchto faktorů spolu s pokračujícími technologiemi vyvolává řadu otázek a vedla ke snaze zajistit základní bezpečí občanů EU. GDPR je reakcí na rychlou digitalizaci a kybernetizaci našeho prostoru. Zda reakce úspěšnou, to ukáže až čas.

Mnohým se může zdát, že se jedná o další regulaci, tedy snahu zase uloupnout kousek naší svobody. Ve skutečnosti se tento krok z pohledu běžného občana jeví jako oprávněná snaha zabezpečit alespoň základní právo svobody jedince, protože snaha monitorovat každý náš krok, ať už vládou nebo korporacemi, je zjevná.

Nařízení GDPR je novátorské i v tom směru, že se netýká jen entit v rámci EU, ale kohokoliv, kdo chce zpracovávat data občanů EU. Firma z Hong Kongu nebo nevládní organizace z USA působící na území Evropské unie tak musí vyhovět požadavkům GDPR stejně jako česká nebo slovenská firma.

1.2.2 Historie ochrany osobních dat

GDPR vychází z původní směrnice EU o ochraně osobních údajů (DPD). Ve svých požadavcích jde dále než HIPAA v USA či jiné legislativní regulace snažící se o ochranu osobních údajů. GDPR je v současné době nejkomplexnější zákonná norma chránící soukromí občanů.

Směrnice o ochraně osobních údajů (DPD) existuje již dvacet let. Stanovuje minimální standard zákona o ochraně údajů v členských státech EU. Česká republika v roce 2000 přijala vlastní zákon týkající se ochrany osobních údajů. Většina států Evropské unie přijala nějakou legislativu řešící problematiku ochrany osobně identifikovatelných informací.

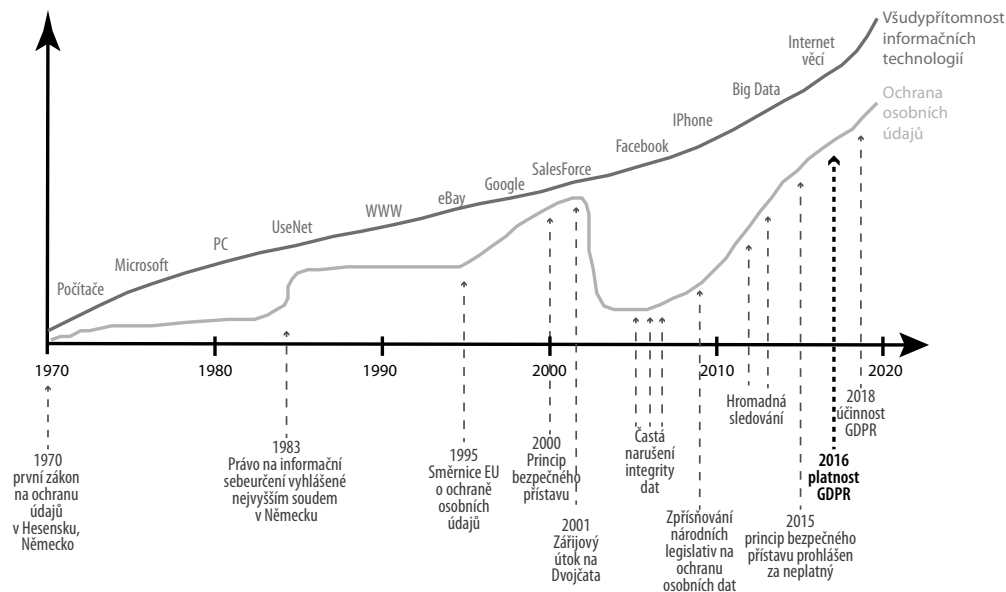
Vývoj technologií je vždy rychlejší než vývoj právních norem. Důležitá je však reakční doba právního systému na technologické změny. Níže je popsána historie vývoje ochrany osobních údajů z hlediska GDPR.

28. leden 1981: Podpis smlouvy o ochraně osob s ohledem na automatické zpracování osobních údajů. Byla podepsána jako Úmluva Rady Evropy č. 108 a vstoupila v platnost dne 1. října 1985. Všech 47 členů Rady Evropy smlouvu ratifikovalo, s výjimkou Turecka.

4. říjen 1995: Evropská směrnice o ochraně osobních údajů (oficiálně: směrnice 95/46 / ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů) byla vytvořena jako základní prvek ochrany soukromí v rámci EU a práva v oblasti lidských práv. Tato směrnice vstoupila v platnost dne 13. prosince 1995 a požadovala od členských států EU, aby do 24. října 1998 provedly příslušná ustanovení ve vnitrostátním právu.

19. květen 2009: Evropská komise zahájila konferenci věnovanou využití a ochraně osobních údajů a zkoumání nových úkolů týkajících se ochrany soukromí. Součástí konference byl i panel věnující se oblasti ochrany osobních údajů v globalizovaném světě se zvýšenou mobilitou a v souvislosti s moderními komunikačními a informačními technologiemi, výměnou dat mezi veřejnými orgány a soukromými společnostmi a mezinárodními přenosy osobních údajů v rámci cloud computingu¹.

¹ **Cloud computing** je model vývoje a používání počítačových technologií založený na internetu. Lze ho také charakterizovat jako poskytování služeb či programů servery dostupnými z internetu s tím, že uživatelé k nim mohou přistupovat vzdáleně, kupř. pomocí webového prohlížeče nebo klienta elektronické pošty.



Obrázek 1 – vývoj technologií v porovnání s vývojem legislativy

1. prosinec 2009: Pracovní skupina zřízená podle článku 29 (WP29)² a pracovní skupina pro politiku a spravedlnost (WPPJ) zveřejňuje dokument „Budoucnost soukromí“³ jako reakci na stanovisko Evropské komise v souvislosti s novými výzvami v oblasti ochrany osobních dat. Tehdy aktuální hlavní principy ochrany osobních údajů jsou považovány za stále platné navzdory novým technologiím a globalizaci. Dokument však zdůrazňuje, že úroveň ochrany osobních údajů v rámci EU lze zvýšit lepším uplatňováním stávajících zásad a legislativy v oblasti ochrany osobních údajů v praxi a postupnou modernizací právního rámce.

4. listopad 2010: Evropská komise stanovuje strategii, jak chránit údaje jednotlivců ve všech oblastech, a to včetně vymáhání práva. S tím omezuje byrokratické požadavky a zaručuje volný pohyb údajů v rámci EU. Znamená to přehodnocení dosavadní politiky a Komise tím aplikuje výsledky veřejné diskuze k revizi evropské směrnice o ochraně osobních údajů.

22. červen 2011: Výbor pro občanské svobody, spravedlnost a vnitřní věci (LIBE)⁴ přijímá návrh komplexního přístupu k ochraně osobních údajů. Klíčovým tématem se stává budoucnost evropského práva v této oblasti a změna stávající směrnice o ochraně údajů 95/46 / ES⁵.

17. listopad 2011: Během zahájení zasedání 35. konference o ochraně soukromí, německého sdružení pro ochranu údajů a ochranu údajů (GDD)⁶, Paul Nemitz oznamuje, že Evropská komise plánuje zavést nařízení, které je přímo aplikovatelné ve všech členských státech EU a bude harmonizovat zákony na ochranu osobních údajů v rámci celé Evropy.

25. leden 2012: Evropská komise navrhuje komplexní reformu pravidel EU ochrany osobních údajů z roku 1995 za účelem posílení práv, zejména v online prostředí. Komise konstatuje, že technologický pokrok a globalizace výrazně změnily způsob, jakým jsou osobní data

² http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

³ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

⁴ <http://www.europarl.europa.eu/committees/cs/libe/home.html>

⁵ <http://www.eurlex.cz/dokument.aspx?celex=31995L0046>

⁶ <https://www.gdd.de/international/english>

shromažďována, zpřístupňována a využívána. Souběžně s návrhem nařízení o obecné ochraně údajů (5853/12)⁷ přijala Komise i směrnici o zpracování údajů za účelem vymáhání práva (5833/12).⁸

21. února 2012: EurActiv⁹ oznamuje, že Spojené státy velmi aktivně ovlivnily průběh projednávání ve snaze ochránit zájmy amerických společností působících v EU. V důsledku tohoto tlaku byl text navržený Komisí výrazně upraven ve prospěch USA a po tomto zjištění návrh nebyl už dále projednáván.

23. březen 2012: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29 (WP29)¹⁰ zveřejnila své stanovisko 01/2012¹¹ jako počáteční příspěvek k diskusi o reformě ochrany osobních údajů. V tomto stanovisku vítá posílení postavení subjektů údajů, posílení odpovědnosti správců a posílení postavení orgánů dohledu, jak na vnitrostátní, tak na mezinárodní úrovni, s potenciálem výrazně snížit stávající roztržičnost a posílit ochranu osobních údajů v celé Evropě.

12. duben 2012: Německý poslanec Evropského parlamentu a Výboru pro občanské svobody, spravedlnost a vnitřní věci (LIBE) Jan-Philipp Albrecht je oficiálně jmenován zpravodajem Evropského parlamentu pro nařízení o obecné ochraně údajů.

2. září 2012: Zveřejňuje Evropský parlament studii nazvanou „Reforming the Data Protection Package“¹², kterou realizovala polská advokátní kancelář a němečtí akademičtí pracovníci z Evropského institutu právních studií. Studie upozorňuje na nutnost zlepšení ochrany subjektů, závažné nedostatky v GDPR týkající se nových technologií a služeb, nesoulad práv spotřebitelů a možnost mezinárodní přenositelnosti údajů.

5. říjen 2012: Pracovní skupina pro ochranu údajů podle článku 29 (WP29)¹³ zveřejnila své stanovisko 08/2012¹⁴ jako další příspěvek k diskusi o reformě ochrany osobních údajů, která se konkrétně zabývá definicí osobních údajů, pojmem souhlas a postupy v přenesené pravomoci.

25. říjen 2012: Rada bere na vědomí současný stav obecného nařízení o ochraně osobních údajů. Během rozpravy je diskutována zejména volba právního nástroje. Některé delegace upřednostňovaly směrnici namísto nařízení, protože by umožnila větší pružnost tam, kde by to bylo potřebné. Jiné delegace však zvolily formu nařízení, tak jak navrhla Komise.

28. leden 2013: Komisařka EU pro spravedlnost a místopředsedkyně Evropské komise Viviane Redingová během Evropského dne ochrany údajů 2013 zdůrazňuje, že žijeme v digitálním světě, v němž mají osobní údaje obrovskou ekonomickou hodnotu. V tomto digitálním světě je třeba, aby evropské podniky mohly využít nové možnosti výpočetní techniky a sdílení informací, ale ne na úkor evropských spotřebitelů. Jednotný a moderní zákon o ochraně osobních údajů pro Evropskou unii proto musí zajistit důvěru a vytvářet prostor pro růst jednotného digitálního trhu.

⁷ <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205853%202012%20INIT>

⁸ <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205833%202012%20INIT>

⁹ <http://euractiv.cz/>

¹⁰ http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

¹¹ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf

¹² <http://www.statewatch.org/news/2012/oct/ep-study-dp.pdf>

¹³ http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

¹⁴ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf

14. květen 2013: London Economics zveřejňuje výsledky nezávislého průzkumu¹⁵, který zadal úřad britského komisaře pro informace, aby pomohl porozumět výzvám, které GDPR staví před podniky a organizace. Z dotazovaných 506 podniků nebylo 87 % respondentů schopno odhadnout pravděpodobné náklady na splnění požadavků navrhovaného nařízení a 82 % respondentů nebylo schopno vyčíslit své současné výdaje na dodržování ochrany osobních údajů.

21. říjen 2013: Výbor pro občanské svobody, spravedlnost a vnitřní věci (LIBE)¹⁶ Evropského parlamentu hlasoval za přijetí kompromisního textu GDPR, který obsahoval několik pozměňovacích návrhů, z nichž některé jsou významné ve srovnání s původním návrhem vypracovaným Evropskou komisí v lednu 2012 (např. výrazně zvýšené sankce, rozšířený územní rozsah, přenosy dat do třetích zemí, omezení profilování, pověřenec pro ochranu osobních údajů). Kompromisní návrh byl přijat převážnou většinou (49 pro, 1 proti a 3 se zdrželi) výboru LIBE, který tak dal mandát zpravodaji Jan-Phillipu Albrechtovi, aby s Radou EU vyjednal kompromisní návrh.

28. leden 2014: Místopředsedkyně EU Viviane Redingová vyzývá k vytvoření nové dohody o ochraně osobních údajů během Evropského dne ochrany údajů v roce 2014 s cílem obnovit důvěru v digitální průmysl obecně a s ohledem na transatlantické toky osobních údajů. Vzhledem k tomu, že některé společnosti a vlády nadále považují ochranu dat za překážku, a ne za řešení výzev v digitálním věku, požaduje, aby se začalo u nejnižšího společného jmenovatele a pokračovalo k vysoké úrovni ochrany osobních údajů.

12. březen 2014: Evropský parlament dává silnou podporu GDPR hlasováním na plenárním zasedání s 621 hlasy pro, 10 proti a 22 zdržujícími se hlasování. V návaznosti na toto rozhodnutí Evropského parlamentu dochází k významnému pokroku v reformě ochrany osobních údajů. Tento krok je považován za nevratný a je chápán jako zajištění efektivnější kontroly osob nad jejich osobními údaji.

10. říjen 2014: Rada EU dosahuje částečné shody na konkrétních aspektech návrhu nařízení, kterým se stanoví obecný rámec EU pro ochranu osobních údajů (zejména kapitola IV. o správci a zpracovateli). Částečná shoda je dosažena za vědomí, že:

- a) nic není dohodnuto, dokud nebude vše dohodnuto;
- b) není dotčeno žádné jiné právo;
- c) předsednictví nedává mandát k zapojení do neformálních dialogů s Evropským parlamentem o tomto textu.

7. ledna 2015: Vydává Jan-Philipp Albrecht, německý poslanec Evropského parlamentu a zpravodaj pro GDPR, varování, že GDPR by mohlo být odloženo až do roku 2016 v důsledku neshod Německa, Francie a Spojeného království. Albrecht varoval, že neschopnost odsouhlasit přijetí GDPR povzbudí a zvýší špehování občanů Evropy bezpečnostními službami.

15. červen 2015: Rada EU dosahuje obecné shody nad GDPR. Obecný přístup představuje politickou dohodu, na jejímž základě může Rada nyní zahájit jednání s Evropským parlamentem s cílem dosáhnout celkové dohody o GDPR.

24. června 2015: Původní návrhy Komise na reformu ochrany osobních údajů byly podrobeny přezkumu a změněny zákonodárci jak v Evropském parlamentu, tak v Radě EU¹⁷. Následovalo setkání zástupců Parlamentu, Rady a Komise v Bruselu a došlo k zahájení takzvaného „dialogu“¹⁸, jehož cílem bylo uzavření dohody o GDPR.

¹⁵ <https://ico.org.uk/media/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf>

¹⁶ <http://www.europarl.europa.eu/committees/cs/libe/home.html>

¹⁷ https://europa.eu/european-union/about-eu/institutions-bodies/council-eu_cs

¹⁸ http://ec.europa.eu/codecision/stepbystep/glossary_en.htm

27. července 2015: Evropský inspektor ochrany osobních údajů Giovanni Buttarelli zveřejnil svá doporučení (stanovisko 3/2015)¹⁹ zákonodárcům EU, kteří vyjednávali o konečném znění GDPR. Spustil mobilní aplikaci na porovnávání nejnovějších textů Komise, Parlamentu a Rady pro tablety a chytré telefony.

27. srpna 2015: Server Politico²⁰ oznámil, že široká průmyslová koalice lobuje v Evropské unii za zrušení článku 43a z návrhu GDPR, který by nutil společnosti k odmítnutí žádostí o osobní údaje z nečlenských zemí. Evropský parlament doplnil návrh o tzv. „Anti-FISA“ klauzuli v návaznosti na zveřejnění informací o sledování Edwarda Snowdena bezpečnostními službami USA. (Rada nezahrnula ustanovení do upřednostňovaného znění nařízení).

9. října 2015: Evropský inspektor ochrany údajů Giovanni Buttarelli aktualizoval své dříve zveřejněné stanovisko ze dne 3. října 2015 o GDPR a zdůraznil důvěru jako nutnou podmínku pro inovativní produkty a služby, které se opírají o zpracování osobních údajů s tím, že nařízení o obecné ochraně osobních údajů musí být příkladem etického přístupu.

12. listopad 2015: V Německu je uveden film „Democracy – Im Rausch der Daten“²¹, který ukazuje vytrvalost a tvrdou práci Viviane Redingové, Jana-Phillippa Albrechta, Ralfa Bendratha a dalších na přijetí legislativního rámce pro ochranu osobních údajů v Evropské unii.

9. prosinec 2015: Během diskuse USA a zemí EU o způsobech, jak zvýšit rychlost a zlepšit rozsah sdílení osobních údajů v důsledku útoků na Paříž, Kalifornii a ruské osobní letadlo, generální prokurátor Loretta Lynch varuje, že plánovaná ochrana osobních dat Evropskou unií může podkopat úsilí o potlačení teroristických útoků omezením transatlantického sdílení informací.

15. prosinec 2015: V trialogu mezi Komisí, Radou a Parlamentem o evropské reformě ochrany osobních údajů dosáhli vyjednávači klíčového bodu, kdy ti, kteří v minulosti zastávali rozdílná stanoviska k různým tématům projednávaným v souvislosti s GDPR dospěli ke shodě i ve směrnici o přenosu údajů pro policejní a soudní účely.

17. prosinec 2015: Výbor pro občanské svobody, spravedlnost a vnitřní věci Evropského parlamentu (LIBE) schválil výsledek třístranných jednání o obecném nařízení o ochraně osobních údajů (GDPR). Převážnou většinou (48 hlasů pro, 4 proti a 4 se zdrželi) výbor LIBE schválil text GDPR včetně ustanovení o jednoznačném, konkrétním a srozumitelném souhlasu, dětech na sociálních sítích, právu na zapomenutí, právu vědět, že vaše údaje byly napadeny, srozumitelnosti jazyka a pokut ve výši až 4 % celkového celosvětového ročního obrátu firem.

18. prosinec 2015: Výbor stálých zástupců (Coreper)²² potvrdil s převážnou většinou (pouze jedním hlasem proti) kompromisní znění schválené Radou, Parlamentem a Komisí dne 15. prosince. Po právně-jazykové revizi těchto textů byl návrh předložen k přijetí Radou a následně Parlamentem. Obecné nařízení o ochraně údajů (a směrnice o předávání údajů pro účely policejní a soudní spolupráce) pravděpodobně vstoupí v účinnost na jaře roku 2018.

21. prosinec 2015: Zveřejňuje Evropská komise na základě dohody, kterou nedávno dosáhl Evropský parlament a Rada, informační list obsahující často kladené otázky a odpovědi týkající se evropské reformy v oblasti ochrany osobních údajů.

28. leden 2016: 47 zemí Rady Evropy, jakož i evropské instituce, agentury a orgány oslavily 10. ročník Evropského dne ochrany osobních údajů. Série událostí věnovaných tomuto výročí zahrnovala konferenci, kterou společně uspořádal Evropský parlament a evropský inspektor ochrany osobních údajů pro úředníky EU ohledně reformy v oblasti ochrany osobních údajů.

¹⁹ https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_en.pdf

²⁰ <http://www.politico.com/>

²¹ <http://www.democracy-film.de/>

²² <http://www.consilium.europa.eu/cs/council-eu/preparatory-bodies/coreper-i/>