

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 | Kamerové 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 pověřence | 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 pověření pro ochranu osobních údajů | 278 |
| 11.1.7 | Pověřenec musí mít osvědčení (certifikát) | 278 |
| 11.1.8 | Obecné nařízení klade na pověření 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 mém 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 |