
Spis treści

1. Co ma norma ISO/IEC 27701 do przetwarzania danych w sieci i kto powinien ją stosować	11
Ogólnie o zabezpieczeniach	11
Normy ISO – co to takiego	12
Rodzina norm 27000	13
Cyberbezpieczeństwo w polskich przepisach	13
KRI i SZBI	15
W jakich przypadkach wdrażać ISO 27701	16
2. Urządzenia mobilne prywatne czy służbowe – które wybrać	17
Plusy i minusy każdego rozwiązania	17
Jak uregulować to w organizacji	18
Gdy urządzenia udostępnia administrator	20
Zdalny dostęp do urządzenia użytkownika a kwestie prywatności	21
Czy można monitorować urządzenia służbowe	23
3. Kiedy będzie wymagane DPIA w związku z przetwarzaniem danych w sieci	25
3 przypadki, gdy wymagana jest DPIA	26
Kto odpowiada za DPIA	27
Co powinien brać pod uwagę oceniający	28
DPIA a oprogramowanie w organizacji	29
Pomocny wykaz UODO	29
4. Jakie rozwiązania przewidzieć w tworzonym oprogramowaniu	33
Nie można zapominać o oczekiwaniach klienta	34
Szyfrowanie – czy rozwiązuje wszystkie problemy.....	35
Należy zapewnić sobie możliwość znalezienia i usunięcia danych	36
Weryfikacja działań użytkowników	37
Uwierzytelnianie dwuskładnikowe – czy warto	38
Czy zewnętrzny usługodawca wchodzi w grę	38
Podstawa prawna przetwarzania danych w aplikacji mobilnej	39
Jak przeprowadzić analizę aplikacji webowych	46

5. Kiedy można korzystać z usług cyfrowych podmiotów zlokalizowanych poza EOG	51
Sprawa Schrems II	51
Specjalne rozwiązania w RODO	52
Standardowe klauzule umowne? Nie zawsze wystarczają	53
Środki uzupełniające według EROD	53
Obowiązek weryfikacji spoczywa na administratorze	54
Krok 1. Zidentyfikuj transfery	55
Krok 2. Zweryfikuj narzędzie	56
Krok 3. Oceń system prawny państwa trzeciego	56
Krok 4. Przyjmij środki uzupełniające	57
A może zmiana regionu przechowywania danych	57
Nowy mechanizm transferów danych z Unii Europejskiej do USA – <i>Data Privacy Framework</i>	58
Lista sprawdzająca dla administratorów danych osobowych (ADO) i podmiotów przetwarzających: Podstawa przekazania danych osobowych do USA, z uwzględnieniem stanu prawnego obowiązującego od 10 lipca 2023 r.	66
Jak zarządzać danymi za pomocą wiążących reguł korporacyjnych	73
Podstawowe informacje o BCR	75
6. Jak korzystać z usług chmurowych według KNF	81
Definicja „chmury” według KNF	81
Jak dostosować swoje działania do komunikatu	84
Analiza ryzyka według KNF	85
Łańcuch outsourcingowy	88
Jak uregulować umowę z dostawcą usług chmurowych	88
7. Usługi chmurowe – kto odpowiada za wyciek danych	89
Odpowiedzialność spoczywa na ADO	89
Co w przypadku chmury zlokalizowanej w państwie trzecim	89
Żądania poszkodowanego	90
Do odpowiedzialności można pociągnąć procesora	91
8. Kto powinien wprowadzić System Zarządzania Bezpieczeństwem Informacji	93
SZBI – co to jest	93

SZBI a RODO	94
Nie tylko dokumentacja ochrony danych	94
Kto wprowadza SZBI	95
SZBI a podmiot przetwarzający	96
9. Jakie rozwiązania w zakresie bezpieczeństwa danych stosować w gamedevie	99
Ochrona danych w gamedevie	99
Jakie dane przetwarza deweloper	100
Rejestr czynności przetwarzania u dewelopera	102
Bezpieczeństwo przede wszystkim	102
Konieczna analiza ryzyka	103
Deweloper musi stosować regułę privacy by design	104
Użytkownik musi otrzymać informacje o przetwarzaniu jego danych	104
Transfer danych do odbiorców	106
10. Czy IOD musi znać się na ochronie danych w sieci	109
Znajomość RODO nie wystarczy	109
Wymagana znajomość praktyki w zakresie cyberbezpieczeństwa	110
IOD musi być świadomy specyfiki organizacji	112
Można korzystać ze wsparcia działu IT	113
11. Jak zapewnić bezpieczeństwo danych podczas wideokonferencji ..	115
Wideokonferencja a przetwarzanie danych	115
Kto jest administratorem danych uczestników wideokonferencji	115
Na jakiej podstawie przetwarzać dane osobowe podczas wideokonferencji	116
Nagrywanie prelegentów	118
Wybór platformy	121
12. Jak realizować obowiązek informacyjny w sieci	123
Treść informacji	123
Czy można skrócić klauzulę	125
Klauzula warstwowa	126
Specyfika danych przetwarzanych w sieci	127

Obowiązek informacyjny a konkurs internetowy	128
Obowiązek informacyjny a e-mail	130
Obowiązek informacyjny a platformy sprzedażowe	131
13. Jak przetestować system IT pod kątem zgodności z RODO?	133
Czy audyt jest obowiązkowy	133
Co składa się na audyt	134
Audyt urzędów i oprogramowania	135
Audyt poczty e-mail	136
Należy przygotować się na wypadek awarii	136
Dokumentacja objęta audytem	136
Personel również można audytować	137
Na koniec raport z audytu	137
14. RODO w e-mailu – jak zapewnić bezpieczeństwo poczty elektronicznej	139
Ocena poziomu zabezpieczeń	139
Bezpieczeństwo w ramach logowania	141
Czy należy szyfrować pocztę	141
Identyfikacja użytkowników	142
Czy obędzie się bez umowy powierzenia	143
Monitorowanie poczty elektronicznej	145
Monitorować można jedynie pocztę służbową	146
Monitorowanie a regulacje w zakładzie pracy	146
Monitorowanie a DPIA	148
15. Polityka prywatności i polityka haseł – czy warto je stosować	149
Polityka prywatności – obowiązek czy zalecane rozwiązanie	149
Nie tylko polityka	150
Tłumaczenie nie jest obowiązkowe	151
Treść polityki	151
Stosowanie plików cookie za zgodą użytkownika	154
Informacja o odbiorcach danych	154
Jak długo przetwarzać dane	156
Prawa podmiotów danych	157
Informacja o zautomatyzowanym podejmowaniu decyzji	157

Polityka prywatności na portalu społecznościowym	158
Jakie zapisy należy zawrzeć w polityce haseł	159
Minimalny poziom bezpieczeństwa hasła	159
Jak konstruować hasła	160
Stawiamy na dłuższe hasła	160
Ograniczony dostęp do konta	161
Zabezpieczenia z wykorzystaniem sprzętu użytkownika	162
Jak uregulować procedury uzyskania dostępu	163
Ewidencja haseł według CNIL	164
16. Na jakiej podstawie przetwarzać dane w postaci odcisków palców pracownika?	165
Przetwarzanie danych szczególnej kategorii	165
Podstawa przetwarzania danych biometrycznych	166
17. Jak zareagować na cyberatak?	167
Krok 1. Działania przygotowawcze	167
Krok 2. Szkolenie personelu	168
Krok 3. Wykrycie naruszenia	169
Krok 4. Ocena naruszenia	170
Krok 5. Wdrożenie zabezpieczeń	173
Krok 6. Wypełnienie dokumentacji	173
18. Jakie są zasady ochrony danych osobowych podczas pracy zdalnej?	175
Środki bezpieczeństwa podczas pracy zdalnej	176
Kontrola ze strony pracodawcy	178
Ochrona danych osobowych pracowników	179
19. Jakie są zasady publikowania wizerunku w sieci	183
Ochrona wizerunku – rozpowszechnianie wymaga zgody	183
Dorozumiana zgoda na rozpowszechnienie wizerunku	184
Opłacony wizerunek może być rozpowszechniany bez zezwolenia	185
Rozpowszechnianie wizerunku bez zgody możliwe w przypadku osoby publicznej	186
Wizerunek osoby stanowiącej jedynie szczegół całości	187

Co grozi za bezprawne rozpowszechnianie wizerunku bez zgody	188
Zdjęcie pracownika na firmowym Facebooku	189
Pracodawca musi mieć podstawę przetwarzania wizerunku pracownika	190
Zgoda na rozpowszechnianie wizerunku na firmowym fanpage'u	190
Co grozi pracodawcy za wykorzystanie wizerunku pracownika bez jego zgody	191
Naruszenie dóbr osobistych pracownika	191
20. Jakie postanowienia zawiera akt o usługach cyfrowych	193
7 nowych obowiązków dla platform internetowych	193
Kto podlega aktowi o usługach cyfrowych	194
Trzy rodzaje usług objętych aktem	195
Obowiązki w akcie usług cyfrowych są stopniowane	197
Każdy dostawca musi wyznaczyć punkt kontaktowy	198
Organizacja interfejsów	199
Zakaz zróżnicowanej ekspozycji treści	199
Wielokrotne pytanie o zgodę	200
Nie można namawiać użytkownika do zmiany decyzji	201
Rezygnacja z usługi musi być łatwa	202
Sprzeciw w sposób zautomatyzowany	202
Ważne wytyczne EROD	203
<i>Privacy by design</i> w akcie o usługach cyfrowych	204
Dodatkowe obowiązki w przypadku umów online	205
Konieczna identyfikacja przedsiębiorcy korzystającego z usług platformy WWW	205
Możliwa identyfikacja elektroniczna	206
Przedsiębiorca musi złożyć dodatkowe oświadczenie	207
Przedsiębiorca może być wezwany do potwierdzenia danych	208
Informacje od przedsiębiorcy objęte poufnością	209
Compliance by design	209
Dostawca może weryfikować spełnienie obowiązku informacyjnego	210
Wykaz aktów prawnych, na które powołano się w publikacji	212