

SPIS TREŚCI

Wstęp	2	Krok 7. Inspektor ochrony danych	31
Krok 1. Zakres stosowania RODO – czy i mnie to dotyczy?	3	IOD – czy to ma sens?	31
Materialny zakres stosowania RODO	3	Obowiązek wyznaczenia IOD	31
Przetwarzanie według RODO	3	Dobrowolne wyznaczenie IOD	32
Dane osobowe według RODO	3	Wyznaczenie wewnętrznego lub zewnętrznego IOD	32
Wizerunek	4	Wytłumaczenie co do wyznaczenia IOD	32
Sposoby przetwarzania danych	4	Zadania IOD	33
Kiedy muszę stosować RODO?	5	Publikacja danych kontaktowych IOD i zgłaszanie ich do organu nadzorczego	33
Wyjątki	6	Krok 8. Prawa osób, których dane dotyczą	35
Terytorialny zakres stosowania RODO	6	Prawo do przejrzystej komunikacji	35
Podstawowe pojęcia: administrator, podmiot przetwarzający i jednostka organizacyjna	6	Prawo do informacji	35
Krok 2. Zaczynij działać	9	Prawo do dostępu do danych	37
Po pierwsze, sięgnij po proste i wiarygodne opracowanie poświęcone RODO	9	Prawo do sprostowania danych	37
Po drugie, porozmawiaj o RODO ze swoimi pracownikami	9	Prawo do usunięcia danych, czyli prawo do bycia zapomnianym	38
Po trzecie, przygotuj odpowiednie procedury	10	Prawo do ograniczenia przetwarzania	38
Po czwarte, zadбай o odpowiednie wyposażenie biura	10	Prawo do przenoszenia danych	38
Po piąte, kontroluj	10	Prawo do sprzeciwu	39
Po szóste, w razie wątpliwości – pytaj	10	Prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu	39
Krok 3. Rejestr czynności przetwarzania	11	Zanim zrealizujesz którekolwiek prawo osoby, której dane dotyczą	39
Czy muszę rejestrować czynności przetwarzania?	11	Krok 9. Naruszenie ochrony danych osobowych	41
Zawartość rejestru	12	Co oznacza naruszenie ochrony danych osobowych	41
Rejestr czynności przetwarzania	12	Obowiązek dokonania zgłoszenia organowi nadzorcemu	42
Rejestr kategorii czynności przetwarzania	12	Co powinno zawierać powiadomienie?	42
Dlaczego czasem muszę prowadzić oba rejestry?	12	Obowiązek powiadomienia osoby, której dane dotyczą	42
Definicja czynności	13	Elementy powiadomienia	42
Wzory rejestrów	13	Krok 10. Sankcje i odpowiedzialność	45
Dodatkowe dane w rejestrach, czyli rejestry rozszerzone	15	Administracyjne kary pieniężne	45
W jakiej formie powinienem prowadzić rejestry i dlaczego muszę je aktualizować?	15	Odpowiedzialność karna	46
Krok 4. Zasady przetwarzania danych osobowych	17	Odpowiedzialność cywilna	46
Zgodność z prawem	17	Odpowiedzialność dyscyplinarna pracowników	46
Rzetelność i przejrzystość	17	Krok 11. Wdrażanie RODO w organizacji	49
Ograniczenie celu i minimalizacja danych	17	Realizacja obowiązku rozliczalności	49
Prawidłowość	18	Odpowiedzialność za ochronę danych osobowych i cykliczny przegląd mechanizmów ochronnych	50
Ograniczenie przechowywania	18	Certyfikacja i kodeksy postępowania	50
Integralność i poufność	19	Krok 12. Kontakty z organem nadzorczym	53
Rozliczalność	19	Prezes Urzędu Ochrony Danych Osobowych (PUODO)	53
Krok 5. Administrator, podmiot przetwarzający i współadministratorzy	21	Zadania i uprawnienia PUODO	53
Instytucja współadministrowania	21	Postępowanie w sprawie naruszeń	54
Jak to tłumaczyć, żeby wytłumaczyć?	21	Krok 13. Dane osobowe w prawie pracy dziś	55
Poszukiwanie podmiotu przetwarzającego	21	Które dane możesz przetwarzać od dawna?	55
Umowa powierzenia danych	22	Monitoring wizyjny	55
Bieżąca współpraca	23	Monitoring poczty elektronicznej	56
Nowe pojęcie: pseudonimizacja	23	Krok 14. Dane osobowe w prawie pracy jutro	57
Współpracy ciąg dalszy	23	Które dane będziesz mógł przetwarzać po zmianie niektórych przepisów Kodeksu pracy?	57
Prawo do kontroli	23	Na co będzie potrzebna zgoda?	57
Dalsze powierzenie danych	24	Krok 15. Regularne sprawdzenia	59
Odpowiedzialność	24	Obserwacja procesów	59
Zakończenie współpracy	25	Po pierwsze, rejestr czynności przetwarzania lub rejestr kategorii czynności przetwarzania	59
Krok 6. Bezpieczeństwo przetwarzania	27	Po drugie, stosowane klauzule informacyjne	59
Dane szczególnie chronione i zwykłe	27	Po trzecie, aktualność zgód	59
Postęp techniczny a bezpieczeństwo IT	27	Po czwarte, zamki w szafkach i zabezpieczenia IT	60
Zasada prywatności w fazie projektowania (<i>privacy by design</i>) i w ustawieniach domyślnych (<i>privacy by default</i>)	27	Po piąte, procedury i upoważnienia do przetwarzania danych	60
Najczęstsze błędy	28	Po szóste, ciągle zdobywanie wiedzy	60
Obszary ryzyka	28	Wykaz przydatnych aktów prawnych	63
Cele zabezpieczeń	29		
Bezpieczeństwo IT jako priorytet	29		
Zapobieganie szkodliwemu oprogramowaniu	29		
Właściwe używanie poczty elektronicznej	29		
Szyfrowanie na co dzień	30		
Zarządzanie uprawnieniami	30		