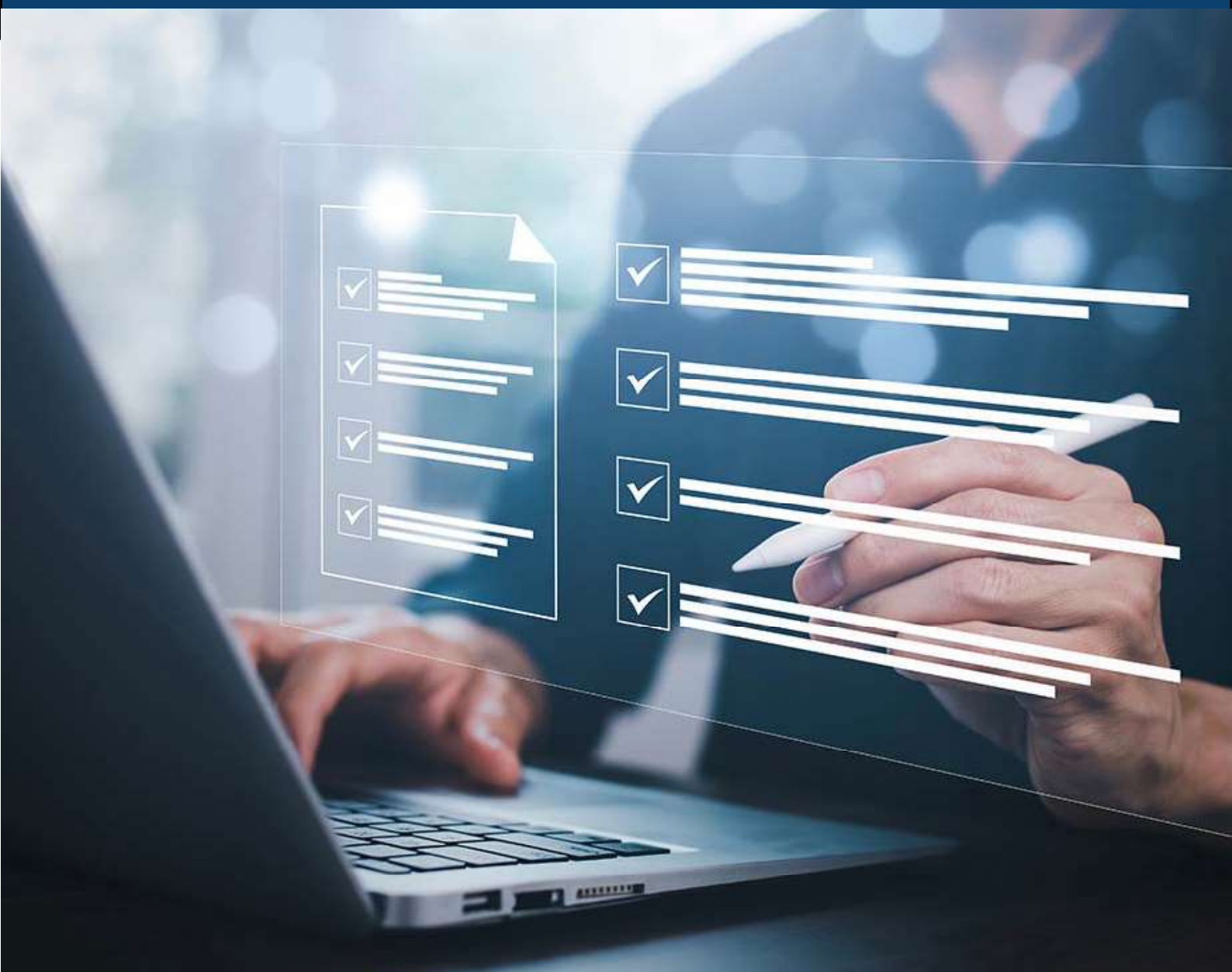


E-BOOK

Listy kontrolne, procedury i instrukcje ODO



OCHRONA DANYCH OSOBOWYCH

Wiedza i Praktyka sp. z o.o.
ul. Łotewska 9A, 03-918 Warszawa
NIP: 526-19-92-256
Redaktor: Anna Śmigulska-Wojciechowska
Segment manager: Agata Eichler
Menedżer produktu: Karolina Jarocho
Koordynacja produkcji: Mariusz Jezierski, Magdalena Huta
Korekta: Zespół
Projekt graficzny publikacji: Piotr Fedorczyk
Skład i łamanie: „Triograf”, Dariusz Kołacz
Drukarnia: KRM Druk
Nr rejestrowy BDO: 000008579
ISBN: 978-83-8409-112-8

Niniejszy e-book chroniony jest prawem autorskim. Przedruk materiałów bez zgody wydawcy jest zabroniony. Zakaz nie dotyczy cytowania publikacji z powołaniem się na źródło. Zaproponowane w niniejszym poradniku wskazówki, porady i interpretacje dotyczą sytuacji typowych. Ich zastosowanie w konkretnym przypadku może wymagać dodatkowych, pogłębionych konsultacji. Publikowane rozwiązania nie mogą być traktowane jako oficjalne stanowisko organów i urzędów państwowych. W związku z powyższym redakcja nie może ponosić odpowiedzialności prawnej za zastosowanie zawartych w poradniku wskazówek, przykładów, informacji itp. do konkretnych przypadków.

1DZ0002
Centrum Obsługi Klienta
Infolinia: od poniedziałku do piątku w godz. 8.00-16.00, tel. 22 518 29 29
Online: formularze.wip.pl
Copyright by Wiedza i Praktyka sp. z o.o. Warszawa 2025

Listy kontrolne, procedury i instrukcje ODO

Lista kontrolna: Sprawdź swoją wiedzę na temat cyberbezpieczeństwa	3
Lista kontrolna dotycząca cyberbezpieczeństwa pomaga ocenić, czy masz odpowiednie zabezpieczenia w systemach informacyjnych, chroniąc dane przed zagrożeniami z sieci.	
Lista kontrolna: Jak zweryfikować podmiot przetwarzający w związku z mającym nastąpić powierzeniem danych osobowych	4
Upewnij się, że współpraca z zewnętrznymi firmami spełnia wymogi ochrony danych, zgodnie z przepisami RODO. Kluczowe jest dokładne sprawdzenie, czy dany podmiot zapewnia odpowiednie środki bezpieczeństwa oraz przestrzega zasad przetwarzania danych osobowych.	
Lista kontrolna: Jak przeprowadzić ocenę skutków ochrony danych w sklepie internetowym w 5 krokach	5
Lista kontrolna dotycząca oceny skutków ochrony danych w sklepie internetowym pomaga przeanalizować potencjalne ryzyka związane z przetwarzaniem danych osobowych i zapewnieniem ich ochrony. W pięciu krokach, takich jak identyfikacja zagrożeń, ocena ryzyka, wdrożenie odpowiednich środków zabezpieczających oraz monitorowanie działań, można skutecznie ocenić wpływ na prywatność użytkowników.	
Lista sprawdzająca: Jakie są terminy aktualizacji dokumentacji dotyczącej ochrony danych osobowych	6
Przepisy nie wskazują, jakie konkretnie dokumenty posiadać oraz jak często je aktualizować, czy też sporządzać. Czasami od tej zasady istnieją wyjątki – np. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.	
Lista kontrolna: Jak stosować pliki cookies na stronie WWW	9
Aby zapewnić zgodność z przepisami, takimi jak RODO i ePrivacy, konieczne jest przeprowadzenie dokładnej analizy, jakie pliki cookies są używane na stronie oraz w jakim celu. Użytkownicy powinni mieć łatwy dostęp do informacji o rodzajach plików cookies, które są zbierane, oraz o sposobie ich wykorzystywania, aby mogli świadomie wyrazić zgodę.	
Lista kontrolna: Jak przeprowadzić ocenę skutków w odniesieniu dla ochrony danych i wdrożyć jej efekty	10
Sprawdź, jak zidentyfikować i ocenić ryzyka związane z przetwarzaniem danych osobowych, a także wskazać odpowiednie środki łagodzące te zagrożenia. Po przeprowadzeniu oceny niezbędne jest wdrożenie działań naprawczych oraz monitorowanie efektywności zabezpieczeń, aby zapewnić zgodność z przepisami o ochronie danych osobowych.	
Procedura usuwania danych osobowych – krok po kroku	11
Procedura usuwania danych osobowych w organizacji obejmuje kilka kluczowych etapów, począwszy od podjęcia decyzji o usunięciu danych, aż po ich faktyczne zniszczenie lub modyfikację.	
Bezpieczeństwo danych osobowych w kontekście dyrektywy NIS2	13
Dyrektywa NIS2 nakłada na organizacje zaliczające się do podmiotów kluczowych i ważnych obowiązki wdrożenia odpowiednich środków zapewniających cyberbezpieczeństwo, w tym polityk zarządzania ryzykiem i procedur dotyczących ciągłości działania.	
Składanie skarg na organy wywiadowcze w USA w związku z przekazanymi do USA danymi osobowymi klientów	14
Sprawdź, jak dochodzić z poziomu krajowego roszczeń z tytułu podejrzenia bezprawnego wykorzystania danych na terenie USA przez tamtejsze organy wywiadowcze. Poniższe wskazówki można stosować niezależnie od wniosków i skarg wobec administratora danych osobowych na mocy prawa krajowego i unijnego.	
Instrukcja alarmowa ochrony danych osobowych	16
Instrukcja definiuje zagrożenia i incydenty, które mogą zagrażać bezpieczeństwu danych osobowych, oraz opisuje procedury reagowania na nie, mające na celu minimalizację skutków i zapobieganie przyszłym ryzykom.	
Instrukcja nadawania uprawnień do dostępu w systemie IT w placówce medycznej	17
Procedura nadawania, zmiany i odbierania uprawnień dostępu do systemów IT w organizacji obejmuje m.in. rejestrację użytkowników, nadanie unikalnych identyfikatorów oraz haseł, a także obowiązek ich okresowej weryfikacji i wyrejestrowania po zakończeniu współpracy.	
Standardy ochrony małoletnich w podmiocie medycznym	18
Standardy ochrony małoletnich w podmiocie medycznym określają zasady rekrutacji personelu, zapewnienia bezpiecznych relacji z małoletnimi, udzielania świadczeń zdrowotnych, postępowania w przypadku krzywdzenia małoletnich oraz procedury szkoleń, aktualizacji i przestrzegania tych standardów.	
Zakres zadań administratora systemów informatycznych (ASI)	20
Administrator systemów informatycznych (ASI) odpowiada za monitorowanie, utrzymywanie i konfigurację systemów informatycznych, zapewniając ich ciągłość działania oraz bezpieczeństwo danych, w tym danych osobowych.	
Zapisy regulaminu konkursu odnoszące się do przetwarzania danych osobowych uczestników konkursu	21
Organizator konkursu zbiera od uczestników dane osobowe, takie jak adres e-mail, imię, nazwisko, stanowisko i firma, a od zwycięzców dodatkowo dane adresowe, numer telefonu, NIP lub PESEL, data urodzenia, dane urzędu skarbowego oraz numer konta.	
Karta szkolenia wstępnego z zakresu ochrony danych osobowych.....	22
Karta szkolenia wstępnego z zakresu ochrony danych osobowych to dokument, który potwierdza ukończenie przez pracownika pierwszego szkolenia dotyczącego zasad ochrony danych osobowych w organizacji. Jest potrzebna w momencie zatrudnienia lub nawiązania współpracy, kiedy pracownik ma dostęp do danych osobowych, aby zapewnić zgodność z przepisami prawa, w tym RODO.	

Lista kontrolna: Sprawdź swoją wiedzę na temat cyberbezpieczeństwa

Lista kontrolna dotycząca cyberbezpieczeństwa pomaga ocenić, czy masz odpowiednie zabezpieczenia w systemach informacyjnych, chroniąc dane przed zagrożeniami z sieci. Regularne aktualizowanie tej listy pozwala na szybkie identyfikowanie luk w zabezpieczeniach i minimalizowanie ryzyka cyberataków.

Środki bezpieczeństwa na stronie WWW	
Czy pamiętasz o aktualizacjach bezpieczeństwa i ważnym oprogramowaniu, jeżeli przechowujesz stronę internetową na własnym serwerze?	☐
Czy przeprowadzasz testy bezpieczeństwa witryny?	☐
Czy pracownicy, logując się na firmową witrynę, stosują bezpieczne hasła?	☐
Czy ograniczyłeś możliwość przesyłania plików bezpośrednio na serwer?	☐
Czy zarejestrowałeś nazwy domenowe brzmiące podobnie do adresu strony WWW? Chodzi m.in. o to, aby nikt nie podszywał się pod dany podmiot.	☐
Czy zadbałeś o stosowanie bezpiecznych i niepowtarzalnych haseł, a także aktywowałeś dwuskładnikowe uwierzytelnianie?	☐
Czy korzystasz z menedżera haseł, który pozwoli tworzyć i automatycznie wprowadzać długie, losowe hasła do serwisów internetowych?	☐
Bezpieczna poczta elektroniczna	
Czy, korzystając z poczty elektronicznej, usuwasz podejrzane wiadomości?	☐
Czy zachęcasz współpracowników, by informowali Cię o takich e-mailach?	☐
Bezpieczeństwo w korzystaniu z drukarek, kopiarek i faksów	
Czy korzystasz z funkcjonalności w zakresie bezpieczeństwa, jakie umożliwiają te urządzenia?	☐
Czy wyłączyłeś możliwość bezpośredniego logowania się do urządzeń z zewnętrznych sieci?	☐
Czy wybierasz takie urządzenia, które mają możliwości szyfrowania i bezpiecznego usuwania danych?	☐
Czy zabezpieczyłeś lub zniszczyłeś przechowywane dane w razie konieczności pozbywania się sprzętu?	☐



Pobierz dokument ze strony dokumentacjaodo.pl lub zeskanuj kod QR



Źródło:

- komunikat Ministerstwa Cyfryzacji w związku z projektem „Kampanie edukacyjno-informacyjne na rzecz upowszechniania korzyści z wykorzystywania technologii cyfrowych” realizowanym we współpracy z Państwowym Instytutem Badawczym NASK

Wszystkie **wzory dokumentów** opublikowane na łamach czasopisma „Ochrona Danych Osobowych” dostępne są również w wersji online na stronie www.dokumentacjaodo.pl.



Lista kontrolna: Jak zweryfikować podmiot przetwarzający w związku z mającym nastąpić powierzeniem danych osobowych

Upewnij się, że współpraca z zewnętrznymi firmami spełnia wymogi ochrony danych zgodnie z przepisami RODO. Kluczowe jest dokładne sprawdzenie, czy dany podmiot zapewnia odpowiednie środki bezpieczeństwa oraz przestrzega zasad przetwarzania danych osobowych.



Pobierz dokument ze strony dokumentacjaodo.pl lub zeskanuj kod QR



Wymogi ogólnego rozporządzenia o ochronie danych (RODO)	Tak	Nie	Uwagi
Czy wdrożył środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa powierzonych danych osobowych odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, w tym posiada: • zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; • zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; • zdolność do regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.			
Czy na żądanie administratora przekaże informacje dotyczących opisu technicznych i organizacyjnych środków bezpieczeństwa zastosowanych do ochrony powierzonych danych.			
Czy korzysta z usług innego podmiotu przetwarzającego?			
Czy zawiera umowy powierzenia z innymi podmiotami przetwarzającymi?			
Czy jest w stanie zrezygnować ze współpracy z którymś ze swoich podmiotów przetwarzających, jeśli administrator danych nie wyrazi na nich zgody?			
Czy pracownicy, którzy będą przetwarzać powierzone dane, mają wydane upoważnienia do przetwarzania danych osobowych?			
Czy osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy poprzez złożenie stosownego oświadczenia?			
Czy zapewni pomoc administratorowi w wywiązaniu się z obowiązku odpowiadania na żądania osoby fizycznej w zakresie wykonywania jej praw przyznanych na mocy RODO – w odniesieniu do powierzanych danych osobowych?			
Czy jest w stanie wspomagać administratora w wywiązaniu się z obowiązków związanych z zabezpieczaniem danych? W jaki sposób? (pole uwagi)			
Czy dysponuje środkami, które pozwalają na usunięcie lub zwrot wszelkich danych osobowych oraz usunięcie ich wszelkich istniejących kopii? Jakże są to środki? (pole uwagi)			
Czy umożliwi administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów?			
Czy jest w stanie informować administratora o naruszeniach ochrony danych osobowych, do których dojdzie w związku z przetwarzaniem danych?			
Czy zapewni pomoc administratorowi w wywiązaniu się z obowiązku zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu oraz zawiadamiania osób fizycznych o naruszeniach w odniesieniu do powierzanych danych osobowych?			
Czy będzie gotowy do pomocy administratorowi w wywiązaniu się z obowiązku przeprowadzenia konsultacji z organem nadzorczym w zakresie powierzanych danych.			
Pytania szczegółowe	Tak	Nie	Uwagi
Czy został wyznaczony inspektor ochrony danych?			
Kto wykonuje zadania dotyczące zapewniania przestrzegania przepisów o ochronie danych osobowych (dotyczy sytuacji w przypadku braku powołania inspektora ochrony danych)? Proszę wskazać stanowisko lub funkcję.			
Czy prowadzi i aktualizuje ewidencję naruszeń ochrony danych osobowych?			
Czy doszło do naruszenia przetwarzania danych osobowych?			
Czy naruszenie zostało zgłoszone do UODO?			
Czy stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO?			