DawnoTemu App

Procedura ochrony przechowywanych lub przekazywanych danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą lub zmianą oraz nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem.

(1) Krok: Identyfikacja i klasyfikacja danych osobowych

Przed rozpoczęciem właściwego procesu ochrony przechowywanych lub przekazywanych danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą lub zmianą oraz nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem koniecznym jest dokonanie identyfikacji i klasyfikacji wszystkich przetwarzanych danych osobowych według ich wrażliwości. Każda kategoria danych (np. dane wrażliwe, dane dotyczące zdrowia) wymaga indywidualnego podejścia w zakresie ochrony i zabezpieczeń. W tym celu wskazanym jest korzystanie z narzędzi do zapobiegania utracie danych do automatycznej klasyfikacji danych i wykrywania nieuprawnionych działań.

(2) Krok: Analiza ryzyka i ocena zagrożeń

Właściwy proces ochrony przechowywanych lub przekazywanych danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą lub zmianą oraz nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem rozpoczyna się od przeprowadzenia szczegółowej analizy ryzyka, która obejmuje identyfikację i ocenę zagrożeń związanych z przechowywaniem, przetwarzaniem i przesyłaniem danych. Należy ocenić możliwe zagrożenia takie jak nieautoryzowany dostęp, przypadkowe zniszczenie czy utrata danych. Analiza powinna być przeprowadzana regularnie, z wykorzystaniem narzędzi takich jak matryce ryzyka i zaawansowane oprogramowania i narzędzia do zarządzania ryzykiem (np. OCTAVE, ISO/IEC 27005). Prawidłowa analiza winna obejmować konsultację z ekspertami ds. cyberbezpieczeństwa i specjalistami ochrony danych, co pozwoli prawidłowo zidentyfikować wszystkie możliwe zagrożenia. Obowiązek stosowania odpowiednich środków technicznych i organizacyjnych wynikających z analizy ryzyka znajduje także odzwierciedlenie w art. 24 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/we (ogólne Rozporządzenie o Ochronie Danych) z dnia 27 kwietnia 2016 r. (Dz. Urz.UE.L nr 119, str. 1), dalej zwane także jako "RODO".

(3) Krok: Środki techniczne i organizacyjne zabezpieczenia danych

Wdrożenie środków technicznych (np. szyfrowanie, systemy kontroli dostępu) oraz organizacyjnych (polityki dostępów, szkolenia) w celu ochrony danych przed przypadkowym zniszczeniem, nieautoryzowaną modyfikacją czy dostępem. Kluczowe jest zapewnienie, że wdrożone środki są odpowiednie do zidentyfikowanych ryzyk. Wskazanym jest stosowanie zasady "najmniejszych uprawnień" (stanowiącej koncepcję cyberbezpieczeństwa, zgodnie z którą użytkownicy otrzymują tylko wystarczający dostęp sieciowy, tzn. uprawnienia użytkownika) do informacji i systemów, których potrzebują do wykonywania swojej pracy, a także regularne przeprowadzanie audytu konfiguracji systemów IT tak, aby móc zidentyfikować potencjalne luki. Wymagania dotyczące wdrożenia odpowiednich środków zabezpieczenia znajdują odzwierciedlenie m. in. w art. 32 RODO.

(4) Krok: Tworzenie i wdrażanie polityki zarządzania incydentami bezpieczeństwa

Polityka zarządzania incydentami powinna szczegółowo opisywać role, obowiązki i standardowe procedury postępowania w przypadku incydentów bezpieczeństwa, a także uwzględniać zawieranie umów o gwarantowanym poziomie świadczenia usług (SLA) w kontekście reagowania na zagrożenia. Skuteczność reakcji zespołu w sposób istotny zwiększają regularne szkolenia i symulacje incydentów.

(5) Krok: Procedury zgłaszania naruszeń i komunikacji z organami nadzoru

Określenie szczegółowych procedur zgłaszania naruszeń ochrony danych do organów nadzoru oraz informowania osób, których dane dotyczą. Procedura powinna uwzględniać określone terminy, role i odpowiedzialności.

(6) Krok: Ochrona danych na urządzeniach mobilnych i w pracy zdalnej

Pożądanym jest także wdrożenie polityki ochrony danych na urządzeniach przenośnych oraz zarządzanie mobilnymi urządzeniami. Szyfrowanie i zdalne zarządzanie danymi są kluczowe w środowisku pracy zdalnej. W tym celu wskazanym jest stosowanie kontroli urządzeń mających dostęp do danych firmowych, a to chociażby w celu zdalnego czyszczenia danych w razie ich utraty.

(7) Krok: Implementacja ochrony danych na poziomie aplikacji

Bezpieczne kodowanie, walidacja danych wejściowych i regularne testy penetracyjne aplikacji są kluczowe dla ochrony danych na poziomie aplikacyjnym. W tym celu należy wdrażać zasady prywatności na każdym etapie rozwoju aplikacji poprzez odpowiednie zaaranżowanie przestrzeni tak, aby była przestrzenią bezpieczną już na tak wczesnym etapie.

(8) Krok: implementacja polityki retencji i minimalizacji danych

Polityka retencji określa czas przechowywania różnych kategorii danych oraz procedury ich usuwania po upływie określonego okresu. Minimalizacja danych ogranicza zbieranie informacji do niezbędnego minimum. W tym celu koniecznym może okazać się stosowanie narzędzi do zarządzania cyklem życia danych, które automatyzują zarządzanie retencją i usuwaniem danych.

(9) Krok: Tworzenie planu zarządzania ciągłością działania i planu odtwarzania po awarii

Plany zarządzania ciągłością działania i odtwarzania/przywracania po awarii powinny obejmować procedury przywracania danych po awarii oraz minimalizacji wpływu incydentów na integralność i dostępność danych. Te plany powinny być regularnie testowane i aktualizowane, aby dostosować je do nowych zagrożeń. Weryfikację skuteczności procedur i lepsze przygotowanie zespołów na sytuacje kryzysowe umożliwić może regularne przeprowadzanie symulacji awarii i testy odzyskiwania danych.

(10) Krok: Backup danych i procedury przywracania danych po awarii

Regularne tworzenie kopii zapasowych i dokładne testowanie procedury odzyskiwania danych po awarii minimalizują ryzyko utraty danych. Tzw. "backupy" powinny być przechowywane w bezpieczny sposób, najlepiej w lokalizacjach zewnętrznych. Wskazanym jest stosowanie takich zasad jak np. "zasada 3-2-1", zakładająca konieczność tworzenia trzech kopii danych, na dwóch różnych nośnikach, w tym jednym poza siedzibą firmy.

(11) Krok: Kontrola dostępu i autoryzacja

System kontroli dostępu powinien zapewniać, że dostęp do danych osobowych mają wyłącznie upoważnione osoby. Należy stosować logowanie dostępu, audyt operacji na danych oraz okresowe weryfikacje i recertyfikację uprawnień użytkowników. Regularne audyty dostępu i recertyfikacja uprawnień użytkowników mają na celu zapewnienie, że pracownicy mają dostęp wyłącznie do danych niezbędnych do wykonywania swoich obowiązków. Przeglądy uprawnień są kluczowe dla minimalizacji ryzyka nieuprawnionego dostępu. Zasady ochrony danych w fazie projektowania oraz domyślna ochrona danych przewidziane zostały m. in. w art. 25 RODO.

(12) Krok: Zarządzanie incydentami bezpieczeństwa

Każdy incydent powinien być identyfikowany, klasyfikowany i dokumentowany zgodnie z jasno określoną polityką. Konieczne jest szybkie powiadamianie organów nadzoru oraz osób, których dane dotyczą, gdy incydent stwarza ryzyko naruszenia ich praw i wolności. Zgłaszanie naruszeń ochrony danych do organu nadzorczego zostało przewidziane m. in. w art. 33 RODO.

(13) Krok: Szyfrowanie i pseudonimizacja danych

Szyfrowanie oraz pseudonimizacja chronią dane przed nieautoryzowanym dostępem, szczególnie podczas przesyłania ich przez sieci publiczne. Pseudonimizacja zmniejsza ryzyko naruszenia prywatności, zastępując dane identyfikacyjne kodami lub numerami identyfikacyjnymi. Praktycznym jest korzystanie z zaawansowanych algorytmów szyfrowania (np. AES-256) i bezpiecznego przechowywania kluczy kryptograficznych. Wyjątki od obowiązku powiadomienia osób, których dane dotyczą, w przypadku zastosowania skutecznych środków ochrony zostały przewidziane w art. 34 ust. 3 RODO.

(14) Krok: Regularne testowanie, ocenianie i mierzenie skuteczności środków bezpieczeństwa

Regularne testy zabezpieczeń, audyty oraz symulacje ataków, takie jak testy penetracyjne i "Red Teaming", są niezbędne do weryfikacji skuteczności środków technicznych i organizacyjnych. W tym celu wskazanym jest wykorzystywanie zewnętrznych audytorów do przeprowadzania niezależnych ocen, które mogą ujawnić luki niezauważone przez wewnętrzne zespoły. Wymóg testowania i oceny skuteczności środków zabezpieczenia został przewidziany m. in. w art. 32 ust. 1 lit. d RODO.

(15) Krok: Zabezpieczenie danych w chmurze i kontrola dostawców usług zewnętrznych

W przetwarzaniu danych w chmurze kluczowe jest zapewnienie, że dostawcy usług spełniają wysokie standardy ochrony danych. W tym celu pomocnym może okazać się regularne audytowanie dostawców (a uprzednio zapewnienie w ramach zawieranych umów odpowiednich warunków dla takich audytów), a to chociażby w celu sprawdzenia sprawdzając polityki szyfrowania i zarządzania kluczami.

(16) Krok: Szkolenia pracowników i podnoszenie świadomości

Regularne szkolenia zwiększają świadomość pracowników na temat ochrony danych i obowiązujących przepisów. Powinny one obejmować zarówno aspekty prawne, jak i techniczne, takie jak rozpoznawanie prób *phishingu*. Obowiązek zapewnienia odpowiednich szkoleń dla personelu przetwarzającego dane przewidziany został m. in. w art. 39 RODO.

(17) Krok: Bezpieczeństwo fizyczne serwerowni i lokalizacji danych

Ochrona fizyczna miejsc przechowywania danych powinna obejmować kontrolę dostępu, monitoring, systemy alarmowe oraz procedury konserwacji kluczowych systemów takich jak zasilanie awaryjne. Praktycznym okazuje się chociażby instalowanie czujników ruchu, kamer oraz stosowanie zasad kontroli dostępu.

(18) Krok: Monitorowanie i audyt wewnętrzny

Regularne monitorowanie przestrzegania procedur ochrony danych oraz audyty wewnętrzne umożliwiają wykrywanie nieprawidłowości i podejmowanie działań korygujących. Audyty powinny obejmować zarówno aspekty techniczne, jak i proceduralne. Wskazanym jest korzystanie z oprogramowania do zarządzania zgodnością, które umożliwi bieżące monitorowanie wszystkich działań związanych z ochroną danych, a także generowanie raportów.

Warszawa, 1 kwietnia 2025 roku.