Dofinansowane przez Unię Europejską

sieć splot wartości

CYFROWA TARCZA PRAWNA

RODO w NGO bez chaosu

Jak bezpiecznie przetwarzać dane i wdrożyć Politykę Ochrony Danych Osobowych

Praktyczny przewodnik dla fundacji i stowarzyszeń

Fundacja LegisLab

Materiał powstał w ramach projektu „Wzmacniamy NGO – Cyfrowa Tarcza Prawna" dofinansowanego ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

Program finansowany jest przez Unię Europejską. Wyrażone opinie i poglądy są wyłącznie poglądami autora (autorów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Komisji Europejskiej. Ani Unia Europejska, ani organ przyznający finansowanie nie mogą ponosić za nie odpowiedzialności.

Wydawca

Fundacja LegisLab, Lubejki 13, 18-106 Turośń Kościelna · sekretariat@fundacjalegislab.pl · www.fundacjalegislab.pl

Spis treści

Jak korzystać z poradnika 4

Polityka w siedmiu krokach 5

Rozdział 1 — Dane osobowe są w codziennej pracy NGO 6

Rozdział 2 — RODO w prostych zasadach 8

Rozdział 3 — Zrób mapę danych, zanim wdrożysz politykę 10

Rozdział 4 — Co powinna zawierać Polityka Ochrony Danych Osobowych? 13

Rozdział 5 — Bezpieczeństwo danych na co dzień 16

Rozdział 6 — Dostawcy, narzędzia i dane poza EOG 18

Rozdział 7 — Incydent to nie powód do ukrywania problemu 20

Rozdział 8 — Wdrożenie Polityki w małej NGO 23

Na koniec 25

Podstawa prawna i źródła 26

Jak korzystać z poradnika

Ten poradnik jest przeznaczony dla fundacji, stowarzyszeń i innych organizacji społecznych, które chcą uporządkować sposób przetwarzania danych osobowych w swojej codziennej działalności.

Nie jest kolejną instrukcją zbierania zgód ani listą trudnych pojęć. Ma pomóc odpowiedzieć na praktyczne pytania: jakie dane organizacja rzeczywiście przetwarza, czy naprawdę ich potrzebuje, kto ma do nich dostęp, gdzie są przechowywane, jak reagować na błąd i jak wdrożyć Politykę Ochrony Danych Osobowych tak, aby działała również po jej podpisaniu.

Na stronie internetowej Fundacji LegisLab dostępny jest edytowalny wzór Polityki Ochrony Danych Osobowych dla NGO oraz dokumenty pomocnicze do jej wdrożenia. Wzór należy dostosować do faktycznej działalności organizacji. Nie powinien być przyjmowany bez uprzedniej analizy procesów, narzędzi, osób mających dostęp do danych i rodzajów danych przetwarzanych przez organizację.

Ważne: poradnik ma charakter edukacyjny i praktyczny. Nie zastępuje indywidualnej porady prawnej ani analizy konkretnego procesu przetwarzania danych. Szczególnej konsultacji mogą wymagać zwłaszcza działania obejmujące dane dzieci, dane o zdrowiu, dane osób w kryzysie, monitoring, duże zbiory danych, profilowanie, narzędzia oparte na sztucznej inteligencji oraz transfer danych poza Europejski Obszar Gospodarczy.

Polityka w siedmiu krokach

1. Rozpoznaj, jakie dane osobowe przetwarza organizacja.
2. Ustal, po co dane są potrzebne i na jakiej podstawie je przetwarzasz.
3. Sprawdź, kto ma dostęp do danych oraz gdzie są one przechowywane.
4. Oceń ryzyka związane z projektami, narzędziami i codzienną pracą.
5. Dostosuj wzór Polityki Ochrony Danych Osobowych dostępny na stronie Fundacji LegisLab.
6. Uporządkuj upoważnienia, poufność, rejestry, klauzule informacyjne i relacje z dostawcami.
7. Przeszkol zespół, reaguj na incydenty i aktualizuj dokumentację po zmianach.

ROZDZIAŁ 1

Dane osobowe są w codziennej pracy NGO

1.1. RODO nie dotyczy wyłącznie dużych organizacji

Fundacja lub stowarzyszenie przetwarza dane osobowe nawet wtedy, gdy nie prowadzi rozbudowanego biura, ma niewielki zespół i realizuje tylko kilka projektów w roku.

Dane pojawiają się między innymi wtedy, gdy organizacja:

- prowadzi nabór uczestników projektu;
- organizuje warsztaty, wydarzenia, szkolenia lub wyjazdy;
- współpracuje z wolontariuszami, ekspertami i podwykonawcami;
- zatrudnia pracowników lub zawiera umowy cywilnoprawne;
- otrzymuje darowizny;
- prowadzi newsletter;
- korzysta z formularzy internetowych, poczty elektronicznej, arkuszy, chmury lub komunikatorów;
- publikuje zdjęcia, nagrania lub relacje z wydarzeń;
- pracuje z dziećmi, osobami z niepełnosprawnościami, seniorami albo osobami w trudnej sytuacji życiowej.

W wielu z tych sytuacji organizacja samodzielnie ustala, po co zbiera dane i jak ich używa. Wtedy działa jako administrator danych osobowych i odpowiada za zgodność przetwarzania z przepisami.

1.2. Dane osobowe to więcej niż PESEL

Dane osobowe to informacje o osobie zidentyfikowanej albo możliwej do zidentyfikowania. Może to być oczywiście imię i nazwisko, PESEL, numer telefonu, adres lub adres e-mail. Danymi mogą być jednak także wizerunek, nagranie głosu, identyfikator uczestnika, adres IP, dane lokalizacyjne albo zestaw informacji, który pozwala ustalić, o kogo chodzi.

Przykład: lista obecności zawierająca imiona i nazwiska uczestników jest zbiorem danych osobowych. Takim zbiorem może być także arkusz z adresami e-mail, folder ze zdjęciami z wydarzenia, skrzynka pocztowa koordynatora projektu czy telefon służbowy z kontaktami do wolontariuszy.

1.3. Mapa danych typowej organizacji

Obszar działania	Przykładowe dane	Co organizacja powinna ustalić
Nabór uczestników	Imię, nazwisko, kontakt, dane o spełnianiu kryteriów projektu	Czy każde pole formularza jest rzeczywiście potrzebne?

Wydarzenia i szkolenia	Listy obecności, dane kontaktowe, informacje organizacyjne	Kto potrzebuje listy i kiedy należy ją usunąć lub zarchiwizować?
Wolontariat	Dane kontaktowe, porozumienie, dyspozycyjność, ewidencja świadczeń	Kto ma dostęp do dokumentacji wolontariusza?
Darowizny	Dane darczyńcy, informacje o wpłacie, korespondencja	Czy dane są używane wyłącznie w celu obsługi darowizny i obowiązków prawnych?
Zatrudnienie i współpraca	Umowy, dane rozliczeniowe, dane kontaktowe, dokumentacja kadrowa	Czy dokumenty są dostępne wyłącznie dla osób, które ich potrzebują?
Newsletter	Adres e-mail, ewentualnie imię, informacja o podstawie kontaktu	Czy osoba może łatwo zrezygnować z komunikacji?
Strona internetowa	Dane z formularzy, cookies, dane analityczne, zapytania e-mail	Czy są odrębne, aktualne informacje dotyczące prywatności i cookies?
Zdjęcia i nagrania	Wizerunek, głos, kontekst wydarzenia	Czy organizacja wie, po co materiał powstaje i gdzie będzie publikowany?

1.4. Dane wymagające szczególnej ostrożności

Niektóre dane mogą ujawniać bardzo wrażliwe informacje o człowieku. Do danych szczególnej kategorii należą m.in. dane o zdrowiu i niepełnosprawności, pochodzeniu rasowym lub etnicznym, przekonaniach religijnych lub światopoglądowych, poglądach politycznych, przynależności związkowej, danych genetycznych, określonych danych biometrycznych oraz seksualności lub orientacji seksualnej.

W działalności NGO takie dane mogą pojawić się na przykład w projektach zdrowotnych, działaniach na rzecz osób z niepełnosprawnościami, inicjatywach skierowanych do konkretnych grup społecznych, programach wsparcia psychologicznego, rekrutacji do projektów finansowanych ze środków publicznych albo przy organizacji wyjazdu wymagającego informacji o potrzebach żywieniowych i zdrowotnych.

Nie należy zbierać takich danych „na wszelki wypadek". Jeżeli ich przetwarzanie jest konieczne, organizacja powinna szczególnie dokładnie określić cel, podstawę prawną, krąg osób mających dostęp, sposób zabezpieczenia i okres przechowywania.

✔️ **CHECKLISTA**

☐ Wiemy, gdzie w naszej organizacji pojawiają się dane osobowe.

☐ Uwzględniliśmy dokumenty papierowe, e-mail, telefony, chmurę i formularze online.

☐ Wiemy, czy przetwarzamy dane szczególnej kategorii lub dane dzieci.

☐ Nie zakładamy, że mała skala działalności zwalnia z zasad ochrony danych.

ROZDZIAŁ 2

RODO w prostych zasadach

2.1. Siedem zasad, które warto znać

RODO nie wymaga od NGO perfekcji ani tworzenia dokumentacji dla samej dokumentacji. Wymaga natomiast, aby organizacja potrafiła uzasadnić, dlaczego przetwarza dane i jak je chroni.

Zgodność z prawem, rzetelność i przejrzystość Dane można przetwarzać tylko wtedy, gdy istnieje właściwa podstawa prawna. Osoba, której dane dotyczą, powinna otrzymać zrozumiałą informację o tym, kto przetwarza jej dane, po co, na jakiej podstawie, jak długo i jakie ma prawa.

Ograniczenie celu Dane zbiera się dla konkretnego, jasno określonego celu. Jeżeli osoba zapisuje się na warsztat, jej danych nie powinno się automatycznie wykorzystywać do wszystkich przyszłych działań organizacji.

Minimalizacja danych Zbieraj tylko dane adekwatne i niezbędne. Jeżeli do zapisania uczestnika wystarczy imię, nazwisko i kontakt, nie pytaj dodatkowo o informacje, których nie potrzebujesz.

Prawidłowość Dane powinny być aktualne. Jeżeli organizacja wie, że dane są błędne albo nieaktualne, powinna je poprawić, ograniczyć ich używanie albo usunąć – zależnie od sytuacji.

Ograniczenie przechowywania Dane nie powinny być przechowywane bezterminowo „na wszelki wypadek". Organizacja powinna ustalić, jak długo potrzebuje ich dla realizacji celu, obowiązków prawnych, rozliczeń albo ochrony przed roszczeniami.

Integralność i poufność Dane należy chronić przed nieuprawnionym dostępem, przypadkowym ujawnieniem, utratą, zniszczeniem i nieuprawnioną zmianą.

Rozliczalność Organizacja powinna umieć wykazać, że działa zgodnie z zasadami. Dlatego znaczenie mają nie tylko deklaracje, lecz także rzeczywiste procedury, rejestry, upoważnienia, szkolenia, decyzje i dokumentowanie incydentów.

2.2. Zgoda nie jest rozwiązaniem na wszystko

Jednym z najczęstszych błędów jest uznanie, że każdą operację na danych da się „załatwić zgodą". Nie zawsze jest to właściwe ani potrzebne.

Przed rozpoczęciem przetwarzania danych należy odpowiedzieć na sześć pytań:

1. Jaki konkretny cel chcemy osiągnąć?
2. Jakiej podstawy prawnej wymaga ten cel?
3. Jakie dane są naprawdę niezbędne?
4. Kto potrzebuje dostępu do danych?

5. Jak długo musimy je przechowywać?
6. Jak przekażemy osobie jasną informację o przetwarzaniu?

Sytuacja	Co należy rozważyć	Błąd, którego warto unikać
Organizacja wydarzenia	Cel organizacyjny, relacja z uczestnikiem, obowiązki rozliczeniowe — zależnie od modelu działania	Zbieranie „zgody na RODO” bez wyjaśnienia celu
Rozliczenie projektu lub księgowość	Obowiązek prawny i obowiązki wynikające z finansowania	Usuwanie dokumentacji potrzebnej do rozliczenia
Obsługa darowizny	Realizacja czynności związanych z darowizną oraz obowiązki prawne	Automatyczne traktowanie darczyńcy jako odbiorcy marketingu
Newsletter	Właściwa podstawa dla komunikacji oraz łatwy mechanizm rezygnacji	Wysyłanie newslettera po zakończeniu projektu bez analizy podstawy kontaktu
Wizerunek z wydarzenia	Odrębna analiza ochrony danych i zasad rozpowszechniania wizerunku	Jedna ogólna zgoda wykorzystana do wszystkich możliwych celów

2.3. Ochrona danych od początku

Dobra praktyka to zaplanowanie ochrony danych zanim ruszy projekt, rekrutacja, nowy formularz lub narzędzie internetowe. Nie trzeba najpierw stworzyć problemu, żeby później próbować go naprawić.

Przed uruchomieniem nowego działania warto zapytać:

- Czy potrzebujemy danych osobowych?
- Czy możemy osiągnąć cel przy mniejszym zakresie danych?
- Czy dane będą obejmowały dzieci albo dane o zdrowiu?
- Czy potrzebny jest nowy formularz, arkusz, narzędzie lub dostawca?
- Czy wiemy, kto będzie miał dostęp do danych?
- Czy ustaliliśmy zasady ich przechowywania i usuwania?
- Czy przygotowaliśmy właściwą klauzulę informacyjną?

Ta zasada jest często określana jako ochrona danych w fazie projektowania i domyślna ochrona danych. Oznacza, że organizacja od początku wybiera rozwiązanie najmniej ingerujące w prywatność, które pozwala osiągnąć założony cel.

ROZDZIAŁ 3

Zrób mapę danych, zanim wdrożysz politykę

3.1. Polityka nie powinna wyprzedzać rzeczywistości

Wzór polityki ochrony danych pomoże uporządkować zasady działania. Najpierw trzeba jednak wiedzieć, jak organizacja działa naprawdę.

Zanim uzupełnisz dokument, przejdź przez wszystkie obszary działalności: projekty, rekrutacje, wydarzenia, wolontariat, darowizny, zatrudnienie, księgowość, stronę internetową, newsletter, media społecznościowe oraz współpracę z dostawcami.

Dla każdego działania ustal podstawowe informacje.

Działanie	Jakie dane są przetwarzane?	Po co?	Kto ma dostęp?	Gdzie dane są przechowywane?	Jak długo?
Nabór uczestników	Dane identyfikacyjne i kontaktowe, dane o spełnianiu kryteriów	Kwalifikacja i organizacja projektu	Osoba prowadząca nabór, koordynator	Formularz, e-mail, folder projektu	Zgodnie z celem, rozliczeniem i zasadami retencji
Warsztat	Lista obecności, dane kontaktowe	Organizacja i rozliczenie działania	Koordynator, osoby uprawnione	Dokumenty papierowe lub plik zabezpieczony	Przez okres wynikający z celu i obowiązków projektu
Wolontariat	Dane kontaktowe, porozumienie, ewidencja	Organizacja współpracy	Koordynator wolontariatu, zarząd	Folder organizacji, dokumentacja papierowa	Przez okres uzasadniony współpracą i roszczeniami
Newsletter	E-mail i informacja o podstawie kontaktu	Wysyłka informacji	Osoba odpowiedzialna za komunikację	System mailingowy	Do rezygnacji, ustania podstawy lub zgodnie z przyjętymi zasadami
Darowizny	Dane darczyńcy i informacje o wpłacie	Obsługa darowizny i księgowość	Zarząd, księgowość	System księgowy, dokumentacja finansowa	Przez okres wymagany przepisami i uzasadniony celem

3.2. Rejestr czynności przetwarzania jest mapą, nie dekoracją

Rejestr czynności przetwarzania pomaga zebrać w jednym miejscu informacje o procesach, w których organizacja używa danych. Dzięki niemu łatwiej odpowiedzieć na pytanie: jakie dane mamy, po co je mamy, kto z nich korzysta, komu je przekazujemy i kiedy powinny zostać usunięte.

Obowiązek jego prowadzenia wynika wprost z art. 30 RODO. Przepis przewiduje wprawdzie wyjątek dla podmiotów zatrudniających mniej niż 250 osób, ale w praktyce z tego wyjątku prawie żadna NGO nie skorzysta w całości. Zwolnienie działa tylko wtedy, gdy jednocześnie: przetwarzanie nie stwarza ryzyka naruszenia praw lub wolności osób, których dane dotyczą, ma charakter sporadyczny oraz nie obejmuje danych szczególnej kategorii ani danych o wyrokach skazujących. Skoro organizacja regularnie prowadzi nabory, zatrudnia lub współpracuje z wolontariuszami, prowadzi newsletter czy pracuje z dziećmi, przetwarzanie przestaje być „sporadyczne" w rozumieniu przepisu — a to oznacza, że rejestr trzeba prowadzić.

Rejestr, zgodnie z art. 30 ust. 1 RODO, powinien zawierać co najmniej: nazwę i dane kontaktowe administratora (oraz IOD, jeśli został wyznaczony); cele przetwarzania; opis kategorii osób, których dane dotyczą, oraz kategorii danych; kategorie odbiorców, którym dane zostały lub zostaną ujawnione (w tym dostawców zewnętrznych); informację o ewentualnym przekazywaniu danych poza EOG; planowane terminy usunięcia poszczególnych kategorii danych; oraz — jeśli to możliwe — ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

W praktyce najwygodniej prowadzić rejestr w formie tabeli, jeden wiersz na jeden proces (np. „nabór uczestników", „newsletter", „rekrutacja pracowników"), zamiast opisywać całą organizację jednym zdaniem — dzięki temu rejestr rzeczywiście odzwierciedla realne działania, a nie ogólną deklarację zgodności.

Wzór rejestru może być dostępny wraz z Polityką Ochrony Danych Osobowych na stronie Fundacji LegisLab. Warto go aktualizować nie tylko raz do roku, lecz także przed rozpoczęciem nowego projektu, wdrożeniem nowego narzędzia lub istotną zmianą dotychczasowego działania.

3.3. Nowy projekt? Zatrzymaj się przed startem

Przed uruchomieniem projektu, naboru, formularza, ankiety, wydarzenia online albo nowego systemu przeprowadź krótką ocenę.

✔️ **Pytania przed startem**

- ☐ Jakie dane chcemy zbierać?
- ☐ Czy wszystkie są niezbędne?
- ☐ Jaki jest cel i podstawa prawna przetwarzania?
- ☐ Czy pojawią się dane dzieci albo dane szczególnej kategorii?
- ☐ Kto będzie miał dostęp do danych?
- ☐ Czy korzystamy z dostawcy zewnętrznego?
- ☐ Czy dane mogą trafić poza EOG?
- ☐ Jak je zabezpieczymy?
- ☐ Jak długo będą przechowywane?
- ☐ Czy uczestnik otrzyma właściwą klauzulę informacyjną?

W pakiecie dokumentów na stronie Fundacji LegisLab może znajdować się karta oceny nowego działania lub procesu przetwarzania. Nie zastępuje ona pogłębionej analizy ryzyka ani oceny skutków dla ochrony danych, jeżeli taka ocena jest potrzebna. Jest natomiast praktycznym narzędziem, które pozwala wychwycić problem przed rozpoczęciem działania.

3.4. Kiedy trzeba zachować szczególną ostrożność?

Szczególnej konsultacji i pogłębionej analizy wymagają zwłaszcza działania obejmujące:

- dane o zdrowiu, niepełnosprawności lub sytuacji kryzysowej;
- dane dzieci i młodzieży;
- ocenę osób albo profilowanie;
- monitorowanie osób na większą skalę;
- łączenie informacji z wielu źródeł;
- nowe technologie, w tym narzędzia wykorzystujące sztuczną inteligencję;
- przetwarzanie dużej liczby danych albo danych szczególnie wrażliwych;
- transfer danych poza Europejski Obszar Gospodarczy.

ROZDZIAŁ 4

Co powinna zawierać Polityka Ochrony Danych Osobowych?

4.1. Polityka jest dokumentem wewnętrznym

Polityka Ochrony Danych Osobowych to dokument, który porządkuje zasady obowiązujące wewnątrz organizacji. Nie jest tym samym co polityka prywatności publikowana na stronie internetowej ani klauzula informacyjna przekazywana uczestnikowi projektu.

Dobra polityka ma pomóc zarządowi, pracownikom, współpracownikom, wolontariuszom i innym osobom mającym dostęp do danych podejmować spójne decyzje. Powinna odzwierciedlać rzeczywisty sposób działania organizacji, a nie być katalogiem ogólnych deklaracji.

Na stronie Fundacji LegisLab można udostępnić edytowalny wzór polityki przeznaczony dla typowej fundacji lub stowarzyszenia. Przed przyjęciem wzoru należy uzupełnić pola oznaczone do uzupełnienia, wybrać właściwe warianty, usunąć nieaktualne fragmenty oraz dopasować dokument do wyników mapowania danych i analizy ryzyk.

4.2. Elementy dobrej polityki

Element polityki	Po co jest potrzebny?	Co organizacja powinna sprawdzić?
Cel, zakres i podstawy	Wyjaśnia, do czego służy dokument i kogo obejmuje	Czy polityka obejmuje papier, e-mail, chmurę, telefony, pracę zdalną i wydarzenia?
Administrator i kontakt	Pozwala ustalić, kto odpowiada za przetwarzanie	Czy podano pełne, aktualne dane organizacji oraz kontakt w sprawach danych?
Role i odpowiedzialność	Rozdziela zadania zarządu, koordynatora, IOD, osób projektowych i osób upoważnionych	Czy każdy wie, za co odpowiada?
Zasady przetwarzania	Przekłada RODO na codzienną pracę	Czy zespół rozumie minimalizację, ograniczenie celu i konieczność zabezpieczania danych?
Procesy i dokumentowanie	Pomaga utrzymać rejestry i wykazać zgodność	Czy rejestr czynności i inne wykazy są aktualne?
Ocena nowego działania	Uczy sprawdzania ryzyka przed startem	Czy nowy formularz, system albo projekt są oceniane przed wdrożeniem?
Dostępy i upoważnienia	Ogranicza dostęp do osób, które go potrzebują	Czy wiemy, kto ma dostęp do skrzynki, dysku, formularzy i dokumentów papierowych?
Środki bezpieczeństwa	Określa podstawowe zasady techniczne i organizacyjne	Czy organizacja stosuje odpowiednie hasła, dostęp, kopie zapasowe i zasady pracy z dokumentami?

Informowanie osób i ich prawa	Zapewnia przejrzystość oraz obsługę wniosków	Czy mamy właściwe klauzule dla uczestników, wolontariuszy, darczyńców i pracowników?
Dane szczególnej kategorii i dane dzieci	Chroni obszary o większym ryzyku	Czy ich zbieranie jest konieczne i ograniczone do niezbędnego zakresu?
Dostawcy zewnętrzni	Porządkuje role podmiotów spoza organizacji	Czy wiemy, kto obsługuje księgowość, hosting, chmurę, newsletter, formularze i wideospotkania?
Transfery poza EOG	Pozwala ocenić ryzyka przy korzystaniu z usług globalnych	Czy sprawdziliśmy, gdzie dostawca przetwarza dane i jakie zabezpieczenia stosuje?
Incydenty i naruszenia	Umożliwia szybką reakcję na błąd lub wyciek	Czy zespół wie, komu i jak szybko zgłosić zdarzenie?
Retencja i usuwanie	Zapobiega niepotrzebnemu przechowywaniu danych	Czy określiliśmy zasady archiwizacji, usuwania i niszczenia dokumentów?
Szkolenia, kontrola i przegląd	Sprawia, że polityka nie zostaje tylko dokumentem	Czy nowe osoby są wdrażane, a dokumentacja jest sprawdzana co najmniej okresowo?

4.3. IOD a koordynator ochrony danych

Inspektor Ochrony Danych jest funkcją przewidzianą przez RODO. Nie każda fundacja lub stowarzyszenie ma obowiązek jego wyznaczenia. Obowiązek może powstać w określonych przypadkach, między innymi przy głównej działalności obejmującej przetwarzanie na dużą skalę szczególnych kategorii danych lub regularne i systematyczne monitorowanie osób na dużą skalę.

Kiedy wyznaczenie IOD jest obowiązkiem, a nie wyborem? Art. 37 RODO przewiduje trzy sytuacje, w których administrator musi wyznaczyć inspektora — wystarczy, że zachodzi choć jedna z nich:

1. przetwarzania dokonuje organ lub podmiot publiczny (poza sądami działającymi jako wymiar sprawiedliwości) — większości NGO to nie dotyczy, chyba że pełnią funkcje zlecone przez administrację publiczną;
2. główna działalność organizacji polega na operacjach, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób na dużą skalę — np. platformy śledzące zachowania dużej liczby użytkowników;
3. główna działalność organizacji polega na przetwarzaniu na dużą skalę danych szczególnej kategorii (zdrowie, orientacja seksualna, przekonania religijne itd.) albo danych o wyrokach skazujących i czynach zabronionych.

Kluczowe jest słowo „główna" i „na dużą skalę". Mała fundacja, która przy okazji projektu zdrowotnego zbiera dane o stanie zdrowia kilkudziesięciu uczestników, zwykle nie spełnia tego progu — bo przetwarzanie takich danych nie stanowi jej głównej działalności ani nie ma charakteru przetwarzania na dużą skalę. Inaczej

może być np. w przypadku organizacji prowadzącej ośrodek terapeutyczny obsługujący tysiące pacjentów rocznie.

Warto też wiedzieć, że IOD nie musi być pracownikiem etatowym — może wykonywać zadania na podstawie umowy o świadczenie usług, a jedna osoba może pełnić tę funkcję dla kilku powiązanych organizacji, jeśli można się z nią łatwo skontaktować z każdej z nich. Jeżeli IOD zostanie wyznaczony (obowiązkowo albo dobrowolnie), jego dane kontaktowe trzeba opublikować i zgłosić do Prezesa UODO.

Mała NGO, która nie ma obowiązku wyznaczenia IOD, może jednak potrzebować osoby, która koordynuje bieżące działania związane z ochroną danych: pilnuje rejestrów, przyjmuje informacje o incydentach, pomaga zespołowi stosować politykę i przypomina o aktualizacjach.

Jeżeli organizacja nie wyznaczyła Inspektora Ochrony Danych, nie powinna nazywać koordynatora „IOD" ani „Inspektorem Ochrony Danych". Trzeba jasno rozróżnić te role.

4.4. Polityka prywatności to inny dokument

Polityka Ochrony Danych Osobowych jest dokumentem wewnętrznym. Polityka prywatności strony internetowej kierowana jest do użytkowników strony i wyjaśnia, jak organizacja przetwarza dane zbierane przez stronę, formularze czy kontakt elektroniczny. Zagadnienia cookies i narzędzi analitycznych również wymagają odrębnego, adekwatnego uregulowania.

Nie należy zakładać, że jedna wewnętrzna polityka rozwiązuje wszystkie obowiązki informacyjne wobec osób, których dane przetwarza organizacja.

ROZDZIAŁ 5

Bezpieczeństwo danych na co dzień

5.1. Dostęp tylko wtedy, gdy jest potrzebny

Jedna z najprostszych i najważniejszych zasad brzmi: osoba powinna mieć dostęp tylko do tych danych, które są jej potrzebne do wykonania konkretnego zadania.

Przykłady:

- Wolontariusz pomagający przy wejściu na wydarzenie może potrzebować listy obecności, ale nie dokumentacji finansowej projektu.
- Osoba przygotowująca newsletter nie potrzebuje dostępu do danych wszystkich uczestników działań.
- Fotograf współpracujący przy wydarzeniu nie powinien otrzymywać pełnej listy kontaktowej uczestników.
- Współpracownik, który zakończył współpracę, nie powinien zachowywać dostępu do skrzynek, dysków, systemów i grup roboczych organizacji.

Dostępy należy nadawać świadomie, przeglądać okresowo i odbierać niezwłocznie po zmianie roli lub zakończeniu współpracy.

5.2. Dziesięć prostych zasad dla zespołu

1. Przetwarzaj dane tylko w zakresie potrzebnym do swoich zadań.
2. Przed wysłaniem e-maila sprawdź adresata i załączniki.
3. Nie przesyłaj danych wrażliwych przez przypadkowy komunikator ani otwarty czat grupowy.
4. Korzystaj z indywidualnych kont. Nie udostępniaj hasła innym osobom.
5. Stosuj silne hasła oraz uwierzytelnianie wieloskładnikowe, gdy narzędzie je oferuje.
6. Blokuj ekran, gdy odchodzisz od urządzenia.
7. Nie przechowuj danych organizacji na prywatnym urządzeniu bez ustalonych zasad bezpieczeństwa.
8. Nie udostępniaj arkusza, folderu ani dokumentu osobie, która nie potrzebuje całego zakresu danych.
9. Niszczenie wydruków wykonuj w sposób uniemożliwiający odczyt danych.
10. Każdy błąd lub podejrzenie błędu zgłaszaj od razu.

5.3. E-mail, chmura, telefon i praca zdalna

W małej organizacji wiele danych znajduje się poza szafą z dokumentami. Są w e-mailu, na telefonach, w folderach współdzielonych, w aplikacjach do zarządzania projektami, na platformach spotkań i w narzędziach do formularzy.

Warto przyjąć kilka podstawowych zasad:

- korzystaj z kont organizacyjnych, gdy jest to możliwe;
- nie używaj jednego wspólnego hasła dla całego zespołu;
- nadawaj dostęp do folderów konkretnym osobom, a nie „każdemu, kto ma link";
- okresowo sprawdzaj, kto ma dostęp do współdzielonych dokumentów;
- włącz uwierzytelnianie wieloskładnikowe przynajmniej dla kluczowych kont;
- aktualizuj programy i systemy;
- wykonuj kopie zapasowe odpowiednie do rodzaju danych;
- ustal, co dzieje się z urządzeniem, skrzynką i plikami po zakończeniu współpracy;
- ostrożnie korzystaj z publicznych sieci Wi-Fi, zwłaszcza przy dostępie do wrażliwych danych.

5.4. Dokument papierowy nadal wymaga ochrony

Listy obecności, umowy, dokumentacja finansowa, oświadczenia, formularze zgłoszeniowe, notatki i wydruki zawierające dane osobowe nie przestają być danymi tylko dlatego, że nie są w komputerze.

Dokumenty papierowe należy przechowywać w miejscu ograniczającym dostęp osób nieuprawnionych. Nie powinny leżeć na stole po zakończeniu spotkania, w samochodzie, w otwartej sali ani w zwykłym koszu na śmieci.

✔️ **CHECKLISTA**

☐ Wiemy, kto ma dostęp do danych i dlaczego go potrzebuje.
☐ Odbieramy dostępy po zakończeniu współpracy.
☐ Korzystamy z indywidualnych kont i odpowiednich haseł.
☐ Sprawdzamy uprawnienia do folderów, formularzy i skrzynek.
☐ Chronimy także dokumenty papierowe.

ROZDZIAŁ 6

Dostawcy, narzędzia i dane poza EOG

6.1. Organizacja rzadko działa całkowicie samodzielnie

Większość NGO korzysta z usług zewnętrznych. Mogą to być między innymi:

- biuro rachunkowe;
- hosting strony internetowej;
- dostawca poczty elektronicznej;
- chmura do przechowywania dokumentów;
- system do newslettera;
- formularz zapisów;
- platforma do wideospotkań;
- firma IT;
- dostawca systemu do zarządzania projektami;
- operator płatności;
- firma obsługująca wydarzenie;
- podwykonawca realizujący część projektu.

Samo korzystanie z zewnętrznej usługi nie jest błędem. Organizacja powinna jednak wiedzieć, jaką rolę pełni dostawca, czy ma dostęp do danych oraz jakie obowiązki trzeba uregulować.

6.2. Nie każdy odbiorca danych jest procesorem

W relacjach z podmiotami zewnętrznymi trzeba rozróżnić co najmniej trzy sytuacje:

- podmiot przetwarza dane w imieniu organizacji i na jej polecenie;
- podmiot otrzymuje dane jako odrębny administrator, ponieważ realizuje własny cel i własne obowiązki;
- strony wspólnie ustalają cele i sposoby przetwarzania danych.

To rozróżnienie wpływa na rodzaj dokumentów i ustaleń potrzebnych w danej współpracy. Nie należy zakładać automatycznie, że każda umowa gospodarcza wymaga identycznej umowy powierzenia przetwarzania danych.

Jeżeli dostawca przetwarza dane w imieniu organizacji, relację należy odpowiednio uregulować. W razie wątpliwości co do roli stron warto ją przeanalizować przed rozpoczęciem współpracy.

6.3. Wybór narzędzia to również decyzja o danych

Przed wdrożeniem nowego systemu lub aplikacji nie pytaj wyłącznie: „Czy to narzędzie jest wygodne, tanie i popularne?". Dodaj pytania:

- Jakie dane będziemy w nim umieszczać?
- Czy potrzebujemy pełnych danych identyfikacyjnych, czy wystarczą dane ograniczone?
- Kto będzie miał dostęp?
- Czy można ustawić różne poziomy uprawnień?
- Czy dostawca zapewnia odpowiednie warunki bezpieczeństwa?
- Czy wiemy, gdzie dane będą przetwarzane?
- Czy narzędzie może przekazywać dane poza Europejski Obszar Gospodarczy?
- Czy po zakończeniu korzystania z usługi można usunąć lub pobrać dane?

6.4. Dane poza Europejskim Obszarem Gospodarczym

Korzystanie z globalnych dostawców chmury, systemów komunikacji, formularzy, narzędzi analitycznych, mediów społecznościowych lub aplikacji opartych na sztucznej inteligencji może wiązać się z przekazywaniem danych poza EOG.

Nie oznacza to automatycznie zakazu korzystania z takich usług. Wymaga jednak świadomego sprawdzenia, na jakiej podstawie dane są przekazywane, jakie zabezpieczenia oferuje dostawca i czy zakres przekazywanych danych jest konieczny.

Im bardziej wrażliwe dane przetwarza organizacja, tym ostrożniej powinna dobierać narzędzia i tym większe znaczenie ma minimalizacja danych.

ROZDZIAŁ 7

Incydent to nie powód do ukrywania problemu

7.1. Czym jest incydent?

Incydent to zdarzenie, które może zagrozić bezpieczeństwu danych. Nie każdy incydent będzie naruszeniem ochrony danych wymagającym zgłoszenia do organu nadzorczego, ale każdy powinien zostać zauważony, oceniony i odpowiednio udokumentowany.

Przykładowe incydenty:

- e-mail z listą uczestników wysłany do niewłaściwej osoby;
- zgubiony telefon z dostępem do poczty organizacji;
- segregator z dokumentami pozostawiony w pociągu;
- folder w chmurze udostępniony publicznie przez nieprawidłowe ustawienia;
- podejrzenie przejęcia skrzynki e-mail;
- były współpracownik, który nadal ma dostęp do dysku organizacji;
- wydruk z danymi wyrzucony do zwykłego kosza;
- wiadomość wysłana do wielu odbiorców z ujawnieniem ich adresów e-mail.

7.2. Pięć pierwszych kroków

1. Zabezpiecz sytuację, o ile możesz to zrobić bez pogłębiania problemu. Przykładowo: zmień hasło, wycofaj błędne udostępnienie folderu albo skontaktuj się z nieprawidłowym odbiorcą wiadomości.
2. Niezwłocznie zgłoś zdarzenie osobie wskazanej w polityce – koordynatorowi, IOD albo zarządowi.
3. Zapisz podstawowe fakty: co się wydarzyło, kiedy, jakie dane mogły być objęte zdarzeniem, ilu osób może dotyczyć problem i jakie działania zostały już podjęte.
4. Nie ukrywaj błędu i nie usuwaj informacji, które mogą pomóc wyjaśnić sprawę.
5. Pozwól organizacji ocenić ryzyko oraz zdecydować o dalszych działaniach.

7.3. Zgłoszenie do Prezesa UODO — obowiązek z art. 33 RODO

Jeżeli naruszenie ochrony danych może powodować ryzyko naruszenia praw lub wolności osób fizycznych, administrator ma obowiązek zgłosić je Prezesowi UODO bez zbędnej zwłoki — w miarę możliwości nie później niż w ciągu **72 godzin** od stwierdzenia naruszenia (art. 33 ust. 1 RODO). Zgłoszenia można zaniechać tylko wtedy, gdy jest mało prawdopodobne, by naruszenie skutkowało ryzykiem dla praw lub wolności osób, których dane dotyczą — a to organizacja musi umieć uzasadnić, a nie po prostu założyć. Jeśli zgłoszenie trafia do organu po upływie 72 godzin, trzeba dołączyć wyjaśnienie przyczyn opóźnienia.

Zgłoszenie musi zawierać co najmniej cztery elementy (art. 33 ust. 3):

- opis charakteru naruszenia, w miarę możliwości z kategoriami i przybliżoną liczbą osób oraz wpisów danych, których dotyczy zdarzenie;
- imię i nazwisko oraz dane kontaktowe IOD albo innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opis możliwych konsekwencji naruszenia dla osób, których dane dotyczą;
- opis środków zastosowanych lub proponowanych, aby zaradzić naruszeniu i zminimalizować jego skutki.

Jeżeli nie da się przekazać wszystkich informacji od razu, RODO dopuszcza ich sukcesywne uzupełnianie bez zbędnej zwłoki — nie trzeba czekać z pierwszym zgłoszeniem, aż sprawa zostanie wyjaśniona w stu procentach. Administrator ma też obowiązek dokumentować każde naruszenie, w tym jego okoliczności, skutki i podjęte działania zaradcze — ta dokumentacja musi pozwolić organowi nadzorczemu zweryfikować, czy organizacja przestrzegała przepisu (art. 33 ust. 5). W praktyce oznacza to, że nawet incydent, który ostatecznie nie wymagał zgłoszenia do UODO, powinien zostać odnotowany wewnętrznie — z opisem, dlaczego uznano ryzyko za nieistotne.

Ocena, czy dane zdarzenie wymaga zgłoszenia, wymaga analizy konkretnej sytuacji; nie należy automatycznie zakładać ani że każde zdarzenie trzeba zgłaszać, ani że żadne nie wymaga reakcji zewnętrznej. Najważniejsze dla osoby z zespołu jest nie samodzielne rozstrzyganie tej kwestii, ale szybkie zgłoszenie zdarzenia wewnątrz organizacji — decyzję o zgłoszeniu do UODO podejmuje osoba odpowiedzialna za ochronę danych albo zarząd.

7.4. Kiedy trzeba zawiadomić same osoby, których dane dotyczą? (art. 34 RODO)

Zgłoszenie do UODO to nie wszystko. Jeżeli naruszenie może powodować **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych, administrator ma dodatkowy obowiązek: bez zbędnej zwłoki zawiadomić o tym również same osoby, których dane dotyczą (art. 34 ust. 1). To sytuacja poważniejsza niż zwykłe zgłoszenie do organu — próg „wysokiego ryzyka" jest wyższy niż próg uzasadniający samo zgłoszenie do UODO.

Zawiadomienie musi być napisane jasnym i prostym językiem oraz opisywać charakter naruszenia, a także zawierać informacje analogiczne do tych z art. 33 ust. 3 lit. b–d: dane kontaktowe IOD lub punktu kontaktowego, możliwe konsekwencje naruszenia oraz zastosowane lub proponowane środki zaradcze.

RODO przewiduje trzy sytuacje, w których zawiadomienie osób **nie jest wymagane** (art. 34 ust. 3):

- organizacja zastosowała odpowiednie zabezpieczenia techniczne (np. szyfrowanie) i te zabezpieczenia obejmowały właśnie te dane, których dotyczy naruszenie — dzięki czemu dane pozostały nieczytelne dla osób nieuprawnionych;

- po naruszeniu organizacja podjęła działania, które wyeliminowały prawdopodobieństwo wysokiego ryzyka dla osób;
- indywidualne zawiadomienie każdej osoby wymagałoby niewspółmiernie dużego wysiłku — wtedy dopuszczalny jest publiczny komunikat lub inny równie skuteczny sposób poinformowania.

Warto pamiętać, że to organ nadzorczy ma ostatnie słowo: jeżeli administrator uzna, że zawiadomienie osób nie jest konieczne, Prezes UODO może i tak zażądać takiego zawiadomienia, jeśli oceni, że naruszenie może powodować wysokie ryzyko (art. 34 ust. 4).

7.5. Dlaczego liczy się szybka informacja?

Największym problemem nie zawsze jest samo zdarzenie. Często większe szkody powoduje zwlekanie: organizacja nie może ograniczyć dostępu, ustalić zakresu problemu, odzyskać dokumentu, zmienić haseł ani ocenić ryzyka w odpowiednim czasie.

Pamiętaj: błąd zgłoszony od razu daje organizacji możliwość reakcji. Błąd ukrywany może narazić ludzi i organizację na znacznie poważniejsze skutki.

ROZDZIAŁ 8

Wdrożenie Polityki w małej NGO

8.1. Przyjęcie dokumentu to środek, nie finał

Polityka Ochrony Danych Osobowych jest potrzebna, ale sama uchwała zarządu nie sprawi jeszcze, że dane będą bezpieczne. Wdrożenie oznacza połączenie dokumentu z realną pracą organizacji.

Poniższy plan można wykorzystać jako harmonogram działań.

Krok 1. Rozpoznaj procesy Zidentyfikuj wszystkie działania, w których organizacja zbiera, przechowuje, wykorzystuje, przekazuje albo usuwa dane.

Krok 2. Ustal cel, podstawę i zakres Dla każdego procesu określ, po co dane są potrzebne, jaka jest podstawa ich przetwarzania, jakie dane są konieczne i jak długo będą przechowywane.

Krok 3. Sprawdź miejsca i narzędzia Zrób listę skrzynek e-mail, folderów w chmurze, komputerów, telefonów, dokumentów papierowych, formularzy, systemów księgowych, platform webinarowych i narzędzi wykorzystywanych przez organizację.

Krok 4. Ustal role i dostępy Sprawdź, kto ma dostęp do poszczególnych danych, komu dostęp jest rzeczywiście potrzebny i co należy zmienić.

Krok 5. Sprawdź dostawców Zidentyfikuj podmioty zewnętrzne, które mają dostęp do danych albo wspierają organizację w ich przetwarzaniu.

Krok 6. Pobierz i dostosuj wzór polityki Skorzystaj z edytowalnego wzoru Polityki Ochrony Danych Osobowych dostępnego na stronie Fundacji LegisLab. Uzupełnij dane organizacji, wybierz właściwe warianty, usuń nieaktualne fragmenty i wpisz rozwiązania odpowiadające rzeczywistym procesom.

Krok 7. Przyjmij politykę i uporządkuj dokumentację Przyjmij politykę w formie właściwej dla organizacji, np. uchwałą zarządu. Uzupełnij rejestry, nadaj upoważnienia, odbierz oświadczenia o poufności oraz przygotuj wymagane informacje dla osób, których dane dotyczą.

Krok 8. Omów zasady z zespołem Nie ograniczaj się do wysłania e-maila z załącznikiem. Omów z zespołem codzienne sytuacje: wysłanie e-maila do grupy, praca na wspólnym dysku, zgubiony telefon, dostęp po zakończeniu współpracy, publikacja zdjęć i nowy formularz zapisów.

Krok 9. Ustal reakcję na incydenty Każda osoba powinna wiedzieć, komu i jak zgłasza problem. Ustal zastępstwo na wypadek nieobecności osoby koordynującej ochronę danych.

Krok 10. Zaplanuj przegląd Dokumentacja nie jest stała. Warto zaplanować regularny przegląd oraz aktualizować ją po uruchomieniu nowego projektu, narzędzia, współpracy albo zmianie w zespole.

8.2. Co znajdziesz na stronie Fundacji LegisLab?

Wraz ze wzorem Polityki Ochrony Danych Osobowych organizacja może korzystać z dokumentów pomocniczych, takich jak:

1. wzór uchwały zarządu wprowadzającej politykę;
2. rejestr czynności przetwarzania danych;
3. wzór upoważnienia do przetwarzania danych;
4. wzór oświadczenia o zachowaniu poufności;
5. ewidencja osób upoważnionych do przetwarzania danych;
6. wzory klauzul informacyjnych dla uczestników projektu, wolontariuszy, darczyńców i pracowników;
7. wzór umowy powierzenia przetwarzania danych dla dostawców zewnętrznych.

Każdy z tych dokumentów powinien zostać użyty w zakresie odpowiadającym działalności organizacji. Pobranie pakietu nie zwalnia z konieczności jego dostosowania.

8.3. Kiedy aktualizować dokumentację?

Przegląd polityki, rejestrów i praktyk warto przeprowadzać co najmniej okresowo, a także wtedy, gdy:

- organizacja uruchamia nowy projekt lub nabór;
- pojawiają się nowe kategorie danych;
- organizacja zaczyna pracę z dziećmi albo danymi o zdrowiu;
- wdrażane jest nowe narzędzie, formularz lub system;
- rozpoczyna się współpraca z nowym dostawcą;
- zmienia się skład zespołu albo zakres jego dostępów;
- wystąpi incydent lub naruszenie ochrony danych;
- zmieniają się istotne przepisy albo sposób działania organizacji.

✔️ CHECKLISTA WDROŻENIOWA

☐ Zmapowaliśmy procesy przetwarzania danych.
☐ Dla każdego procesu ustaliliśmy cel, zakres, dostęp i okres przechowywania.
☐ Sprawdziliśmy narzędzia, chmurę, pocztę, formularze i dokumenty papierowe.
☐ Ustaliliśmy role, upoważnienia i zasady poufności.
☐ Zidentyfikowaliśmy dostawców oraz oceniliśmy ich rolę.
☐ Dostosowaliśmy wzór polityki dostępny na stronie Fundacji LegisLab.
☐ Przyjęliśmy politykę i uporządkowaliśmy dokumentację.
☐ Zespół wie, jak reagować na incydent.
☐ Wyznaczyliśmy termin kolejnego przeglądu.

Na koniec

Bezpieczne przetwarzanie danych nie polega na zbieraniu jak największej liczby zgód ani na tworzeniu dokumentów, których nikt później nie używa. Polega na świadomym podejmowaniu prostych decyzji: czy dane są potrzebne, kto powinien je widzieć, gdzie można je przechowywać, kiedy trzeba je usunąć i co zrobić, gdy wydarzy się błąd.

Polityka Ochrony Danych Osobowych pomaga te decyzje uporządkować. Nie zastępuje jednak uważności zespołu, właściwie skonfigurowanych narzędzi, ograniczenia dostępów ani szybkiej reakcji na problem.

Pobierz ze strony Fundacji LegisLab edytowalny wzór Polityki Ochrony Danych Osobowych oraz dokumenty pomocnicze. Następnie dostosuj je do swojej organizacji, jej projektów, osób zaangażowanych w działania i narzędzi, z których rzeczywiście korzysta.

Dobra ochrona danych jest częścią zaufania. Uczestnik projektu, wolontariusz, darczyńca, pracownik i partner organizacji powinni móc liczyć na to, że ich dane są traktowane z należytą starannością.

Podstawa prawna i źródła

Najważniejsze akty prawne

- **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r.** (Dz. Urz. UE L 119 z 4.05.2016, str. 1, ze zm.) 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 – RODO), w szczególności art. 5, 6, 9, 12--22, 24--25, 28, 30, 32--35, 37 i 44--49.
- **Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych** (t.j. Dz. U. z 2019 r. poz. 1781, ze zm.).
- **Ustawa z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej** (Dz. U. poz. 1221), obowiązująca od 10 listopada 2024 r. – zastąpiła Prawo telekomunikacyjne z 2004 r.; reguluje m.in. zasady używania plików cookies, marketingu bezpośredniego i przesyłania niezamówionych informacji handlowych drogą elektroniczną.
- **Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną** (t.j. Dz. U. z 2024 r. poz. 1513) – w zakresie, w jakim określa obowiązki informacyjne usługodawców świadczących usługi online oraz wymogi dotyczące regulaminów tych usług.
- **Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy** (t.j. Dz. U. z 2025 r. poz. 277, ze zm.) – w zakresie dotyczącym przetwarzania danych osobowych pracowników i kandydatów do pracy, dokumentacji kadrowej oraz obowiązków pracodawcy wynikających ze stosunku pracy.
- **Ustawa z dnia 29 września 1994 r. o rachunkowości** (t.j. Dz. U. z 2023 r. poz. 120, ze zm.) oraz przepisy podatkowe – w zakresie, w jakim określają minimalne okresy przechowywania dokumentów finansowych i księgowych organizacji.
- **Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie** (t.j. Dz. U. z 2024 r. poz. 1491, ze zm.).
- **Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny** (t.j. Dz. U. z 2026 r. poz. 795), w zakresie ochrony dóbr osobistych.
- **Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych** (t.j. Dz. U. z 2025 r. poz. 24), w szczególności art. 81 – w zakresie rozpowszechniania wizerunku.

Materiały pomocnicze

- Materiały Urzędu Ochrony Danych Osobowych dotyczące obowiązków administratorów, naruszeń ochrony danych, bezpieczeństwa i praw osób, których dane dotyczą.
- Aktualne teksty aktów prawnych dostępne w Internetowym Systemie Aktów Prawnych.

- Oficjalny tekst RODO dostępny w serwisie EUR-Lex.
- Materiały dotyczące cyberbezpieczeństwa i dobrych praktyk dla organizacji społecznych, po uprzednim sprawdzeniu ich aktualności i źródła.

Stan prawny na dzień 31 sierpnia 2026 r.