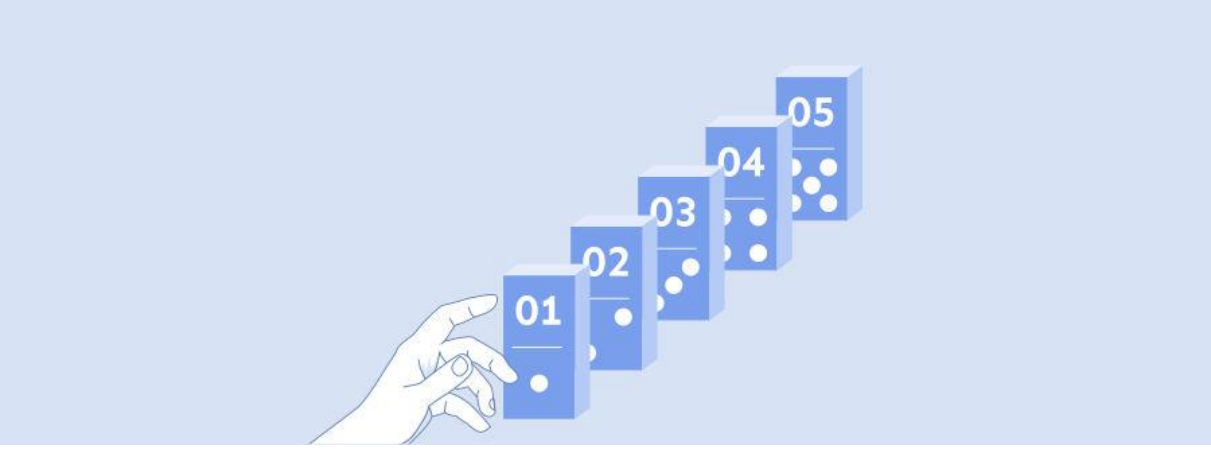


RODO w praktyce, czyli jak zrozumieć RODO w 15 minut

Daję sobie 15 minut, na to, żeby w prosty i przejrzysty sposób wyjaśnić *Ci / Twojemu Zarządowi / szefowi / szefowej / zespołowi* (niepotrzebne skreślić) na czym polega RODO w praktyce.

Brzmi jak *mission impossible*?

W końcu treść Rozporządzenia liczy sobie 99 artykułów i 173 motywy preambuły (tak, je też trzeba przeczytać :). Do tego polska ustawa o ochronie danych osobowych, kilkadziesiąt ustaw "towarzyszących" regulujących zasady ochrony danych w danych branżach. Na deser wytyczne polskiego Urzędu Ochrony Danych Osobowych (UODO), Grupy Roboczej, czy aktualnie Europejskiej Rady Ochrony Danych Osobowych (EROD). A wszystko to podane w ciężęęężkim prawniczym języku.

Nieciekawa perspektywa? Właśnie dlatego warto popatrzeć na RODO z innej, szerszej perspektywy. Z perspektywy która sprawi, że w Twojej głowie z chaosu i rozsypanych RODO-puzzli ułoży się uporządkowany i logiczny obraz systemu ochrony danych osobowych, który musisz wdrożyć w swojej organizacji.

W omówieniu RODO 15 minut, czyli we wspomnianym *mission impossibl*e, pomoże mi nasza autorska koncepcja V filarów. Nie znajdziesz jej ani w tekście RODO ani wytycznych Regulatora, ale gwarantuję Ci, że będzie dla Ciebie bardzo pomocna w zrozumieniu na czym polega ochrona danych osobowych.
Gotowi? No to czas start!

RODO w praktyce, czyli podział na V filarów

System ochrony danych osobowych możemy podzielić na 5 filarów:

1. **Legalność**.
2. **Świadomość**.
3. **Zabezpieczenia.**
4. **Obowiązki względem regulatora (UODO).**
5. **Prawa osób, których dane są przetwarzane.**

Każdy filar składa się z pewnych elementów, które omówię w dalszej części artykułu.

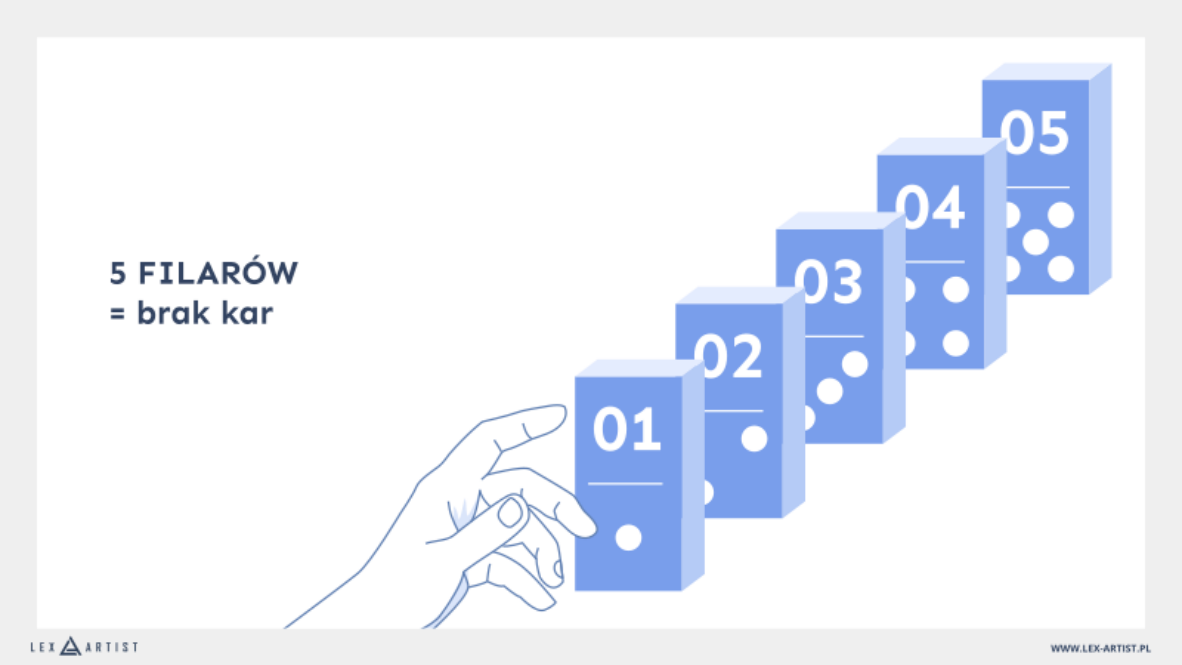
Zanim jednak zacznę – **bardzo ważna uwaga**. Każdy z tych filarów jest równie ważny i każdy z nich powinien zostać wdrożony w Twojej firmie, czy organizacji. Przykładowo – możesz zainwestować miliony złotych w doskonałe zabezpieczenia IT.

Co z tego, skoro nie zadbasz o inny filar, czyli świadomość? Nawet najlepsze zabezpieczenia IT nie uchronią Cię przed naruszeniami RODO, jeśli pracownicy nie wiedzą jak z nich korzystać. Na przykład udostępniają przez telefon dane osobowe niezweryfikowanym odbiorcom, czy wysyłają życzenia świąteczne do swoich

kontaktów w **kopii odkrytej**. Jest to bardzo częsta przyczyna naruszeń ochrony danych osobowych.

Z naszego doświadczenia wynika, że znacznie lepiej zadbać w sposób zrównoważony o każdy z pięciu filarów, niż skupiać się tylko na jednym czy dwóch.

Jeśli jeden z filarów nie będzie w ogóle funkcjonował (czyli metaforycznie przewróci się) – to jak upadająca kostka domina, pociągnie za sobą kolejne filary.



Filar I – Legalność

Jeśli chcesz osiągnąć zgodność z RODO w pierwszym filarze, musisz odpowiedzieć sobie na kluczowe pytanie:

*Czy przetwarzam dane osobowe **LEGALNIE?***

Na pierwszy filar składają się następujące obowiązki:

- przesłanki legalności przetwarzania danych osobowych,
- zasady ogólne oraz
- przekazywanie danych osobowych

Przesłanki legalności przetwarzania danych osobowych

Za każdym razem kiedy przetwarzasz jakieś dane osobowe (np. pracowników, kontrahentów, klientów, subskrybentów newslettera) musisz spełnić **PRZYNAJMNIEJ** jedną tzw. przesłankę legalności.

Przesłanka legalności to jakby zielone światło, które umożliwia Ci legalne przetwarzanie danych osobowych.

Praktyczne przykłady? Proszę bardzo:

- Przetwarzasz dane **pracowników** w celu zatrudnienia? Powołaj się na przesłanki realizacji umowy oraz obowiązku prawnego wynikającego z Kodeksu Pracy (jeśli zatrudniasz na podstawie umowy o pracę).
- Przetwarzasz dane **klienta** w celu realizacji zamówienia? Bazuj na przesłance realizacji umowy.
- Przetwarzasz dane **potencjalnego klienta** w celach marketingowych? Powołaj się na przesłankę prawnie uzasadnionego interesu.
- Chcesz przetwarzać **dodatkowe dane osobowe klienta**, które nie są niezbędne do realizacji zamówienia, czy umowy? Uzyskaj zgodę na przetwarzanie danych osobowych.

Wszystkie przesłanki legalności dla przetwarzania danych osobowych **zwykłych** są wymienione w art. 6 RODO, a dla szczególnych kategorii danych (tzw. danych wrażliwych) – w art. 9 RODO.

Zasady ogólne RODO

Jeżeli przetwarzasz dane osobowe, musisz to robić w zgodzie z zasadami wynikającymi z RODO. Wymienię tutaj dwie zasady przysparzające najwięcej problemów przedsiębiorcom i instytucjom publicznym. Są to zasady:

- minimalizacji
- ograniczenia czasowego

Zasada minimalizacji wymaga od nas, żebyśmy zbierali (przetwarzali) wyłącznie tyle danych osobowych, ile jest absolutnie konieczne do osiągnięcia celu przetwarzania. Nic więcej! Nie możemy np. poprosić subskrybenta o podanie numeru PESEL przy zapisie na newsletter. Nawet jeśli subskrybent wyrazi na to zgodę! Nie ma przecież logicznego wytłumaczenia w jakim celu administratorowi

mogłyby być potrzebne tak szczegółowe dane na potrzeby wyłącznie wysyłki newslettera.

Zasada ograniczenia czasowego – możemy przechowywać dane (a więc przetwarzać, ponieważ przechowywanie danych jest formą ich przetwarzania), wyłącznie tak długo, jak jest to konieczne lub na ile wynika to z przepisów prawa. W skrócie – musisz opracować i wdrożyć zasady retencji – cyklicznego i regularnego czyszczenia swoich baz danych z niepotrzebnych już rekordów. Pamiętaj, żeby w razie konieczności potwierdzać usuwanie większych ilości danych osobowych specjalnymi protokołami.

Przekazywanie danych osobowych

Ostatni z kluczowych elementów filaru legalności to przekazywanie danych osobowych. Możemy wyróżnić dwa rodzaje przekazywania danych:

- powierzenie
- udostępnienie

Jeśli "wypożyczasz", czyli powierzasz dane osobowe zewnętrznemu podmiotowi (np. w ramach outsourcingu kadr, plac, IT, hostingu, księgowości, wysyłki newsletterów), **masz obowiązek** podpisać z tym podmiotem specjalną umowę tzw. powierzenia przetwarzania danych osobowych.

Jeśli przekazujesz dane osobowe w formie udostępnienia (np. do ZUS, policji, sądu, US), rób to zawsze w oparciu o konkretną przesłankę legalności. Pamiętaj przy tym o zachowaniu wszelkich środków ostrożności tak, aby w trakcie przekazywania danych nie doszło np. do ich wycieku.

02 Filar II – Świadomość

Chodzi oczywiście o świadomość obowiązków wynikających z RODO w Twoim zespole. Z naszego doświadczenia wynika, że jest to jeden z najczęściej pomijanych filarów. Bardzo niesłusznie.

Dlaczego? Jak wynika z badań (np. statystyk Związku Firm Ochrony Danych Osobowych ZFODO), najczęstszą przyczyną incydentów RODO nie są ataki hakerów, czy kradzieże, a **błąd ludzki**. Błąd naszego pracownika, kolegi, koleżanki z zespołu.

Jak sobie z tym radzić? Oczywiście szkolenia, szkolenia i jeszcze raz szkolenia! Mogą to być e-learningi. Możesz zadbać o świadomość zespołu w formie szkoleń stacjonarnych. A może warto spróbować broszur, czy plakatów informacyjnych? Może być to oczywiście kombinacja wszystkich powyższych metod.

Zminimalizuj ryzyko naruszenia RODO w Twojej organizacji – przeszkól zespół.

Zależy Ci na tym aby Twoi pracownicy otrzymali certyfikat i poznali praktyczną wiedzę z zakresu RODO zamiast nużących regułek?

Sprawdź nasze interaktywne szkolenia e-learningowe.

SPRAWDŹ

Budując świadomość pamiętaj, że szkolenia muszą być maksymalnie efektywne, tzn. podane w prostej, przejrzystej i czytelnej formie! Nie wystarczy przekazać pracownikowi treści RODO z poleceniem: masz, przeczytaj :). O zgrozo kilka z audytowanych przez nas organizacji prowadziła taką formę "szkoleń".

Gwarantuję, że zadziała to na pracownika lepiej niż jakikolwiek środek nasenny. Gwarantuję też, że większość pracowników tego nie przeczyta. A nawet jeśli przeczyta, to nie zrozumie. Co jeszcze mogę zagwarantować? Że w razie kontroli Urzędu Ochrony Danych Osobowych, czy Administratora powierzającego do

Twojej organizacji dane osobowe, taka forma "szkolenia" nie zostanie zaakceptowana.

Filar III – Zabezpieczenia

To ten filar o którym administratorzy najczęściej pamiętają. Ale czy na pewno poprawnie go interpretują? Czy pamiętają o wszystkich jego elementach?

Nie zaskoczę Cię, jeśli odpowiem, że **NIE** :).
Na filar zabezpieczeń składają się bowiem **trzy elementy**:

1. **Zabezpieczenia IT** – backupy, firewalle, rozliczalność użytkowników, polityki haseł, bezpieczeństwo infrastruktury, szyfrowanie dysków, VPN, itd. RODO nie proponuje nam żadnego konkretnego minimum bezpieczeństwa. Każdy administrator danych ma obowiązek stosowania **adekwatnych** środków bezpieczeństwa. W skrócie – im więcej, im bardziej wrażliwych danych przetwarzasz i im większe jest ryzyko ich wycieku / utraty, tym bardziej zaawansowane zabezpieczenia IT powinieneś/naś wdrażać.

2. **Zabezpieczenia fizyczne** – czyli wszystkie bariery fizyczne, jakie stawiamy osobom nieuprawnionym jakie stawiamy przed dostępem do danych osobowych. Mogą to być np. drzwi zamykane na klucz, systemy kontroli dostępu SKD, szafy zamykane na klucz, portiernia, monitoring. Podobnie jak w przypadku zabezpieczeń IT – RODO nie wprowadza tutaj minimalnego standardu zabezpieczeń jakie należy stosować.

3. **Zabezpieczenia organizacyjne** – czyli procedury, procedury i jeszcze raz procedury. Nie zrozum mnie źle – jestem jak najdalszy od ubierania WSZYSTKIEGO w procedury i tworzenia 500 stronicowych dokumentów, których jedyną rolą jest zbieranie kurzu w szafie. Prawda jest jednak taka, że jeśli przetwarzamy dane osobowe na nieco większą, niż mikro skalę, to musimy opracować swojego rodzaju instrukcje postępowania z danymi osobowymi.

Co konkretnie powinniśmy opracować i wdrożyć? Np. procedurę nadawania i ewidencjonowania upoważnień do przetwarzania danych osobowych, procedurę reagowania na naruszenia ochrony danych, rejestry czynności przetwarzania i rejestry kategorii czynności przetwarzania. Wszystko to najlepiej "ubrać" w jeden, spójny dokument – Politykę ochrony danych.

04 Filar IV – Obowiązki względem regulatora (UODO)

Podstawowe obowiązki, jakie RODO nakłada na każdego* przedsiębiorcę, czy instytucję to:

- Raportowanie o naruszeniach ochrony danych osobowych. Masz na to tylko 72 godziny! Naruszenia możesz zgłaszać elektronicznie, za pośrednictwem specjalnego portalu.

UWAGA! Nie zachęcam do "zamiatania pod dywan" naruszeń ochrony danych osobowych. Może się to szybko obrócić przeciwko Tobie!

- Raportowanie o powołaniu, odwołaniu lub zmianie na stanowisku Inspektora Ochrony Danych osobowych. Masz na to tylko 14 dni. Zgłoszenia również dokonasz elektronicznie.

- Konsultacje, w sytuacjach, kiedy ocena skutków dla ochrony danych, wskaże, że przetwarzanie przez Ciebie danych osobowych powodowałoby wysokie ryzyko naruszenia praw i wolności podmiotów danych, gdybyś nie zastosował środków w celu zminimalizowania tego ryzyka. Konsultacje powinieneś przeprowadzić jeszcze przed rozpoczęciem przetwarzania!

*A co jeśli nie masz obowiązku powołania Inspektora Ochrony Danych? NIC :). Na szczęście nie musisz zgłaszać do żadnego urzędu faktu NIE powołania IOD. Bez przesady:)

Filar V – Prawa osób, których dane są przetwarzane

Każdej osobie, której dane przetwarzasz przysługuje szereg praw. M.in. prawo do:

- Informacji (tzw. obowiązek informacyjny);
- Wycofania zgody na przetwarzanie danych;
- Przenoszenia danych;
- Bycia zapomnianym;
- Dostępu do swoich danych;
- Sprostowania;
- Ograniczenia przetwarzania;
- Prawo do sprzeciwu.

Zapamiętaj dwie kluczowe informacje:

- Jednym z najczęściej zaniedbywanych praw osób, których dane są przetwarzane jest prawo do informacji.

Na czym polega? W skrócie – osoba, której dane osobowe przetwarzamy ma prawo wiedzieć kto, w jakim celu, przez jaki czas i na jakiej podstawie będzie przetwarzał jej dane osobowe.

Obowiązek informacyjny zrealizujesz za pomocą tzw. klauzuli informacyjnej. Zamieszczaj ją wszędzie tam, gdzie zbierasz dane osobowe. Szczególnie przy wszelkiego rodzaju formularzach na stronie internetowej.
Pamiętaj, że strona internetowa jest Twoją wizytówką i BARDZO łatwo jest udokumentować brak wywiązywania się przez Ciebie z obowiązku informacyjnego. Wystarczy, że ktoś wykona *print screen* Twojej strony internetowej niezawierającej odpowiedniej klauzuli informacyjnej, a następnie prześle skargę do UODO. Kłopoty gwarantowane.

- Pierwsza w Polsce, niemal milionowa kara finansowa została nałożona właśnie z tytułu niewłaściwego wywiązywania się z obowiązku informacyjnego!

Zachęcam Cię do zapoznania się z rejestrem kar UODO jaki prowadzimy. Jest to kopalnia wiedzy na temat tego kto, kiedy i za co został ukarany. Każda kara jest skrótowo opisana i opatrzona komentarzem naszych ekspertów. Dzięki czemu znacznie łatwiej będzie Ci wyciągnąć praktyczne wnioski dla Twojej organizacji.

Podsumowanie

Iiiiiiiiiiiiiii... to by było na tyle :).

Widzisz? RODO wcale nie jest takie straszne jak je malują :). Zachęcam Cię gorąco do tego, żeby już DZIŚ podjąć wyzwanie uporządkowania tematu RODO w swojej firmie, czy organizacji.

Pomożemy!

Jeśli nie wiesz od czego zacząć, skorzystaj z "pomocy dydaktycznych":

- z naszego bloga – wiadomo :). W artykule, przy opisie każdego filaru, znajdziesz linki prowadzące do artykułów objaśniających w szczegółach jak opracować dany element systemu ochrony danych osobowych.
- zapraszamy Cię też na nasz trzydniowy kurs online w czasie którego tłumaczymy prostym i przystępnym językiem jak wdrożyć RODO w firmie, czy organizacji. Najbliższe terminy i program szkolenia znajdziesz tutaj.
- z pomocy naszych ekspertów którzy przeprowadzą dla Ciebie audyt i wdrożenie RODO, przeszkolą zespół, czy udzielą wsparcia konsultacyjnego. Zobacz co możemy dla Ciebie zrobić tutaj.

Bądź na bieżąco – dołącz do naszych mediów

Co jeszcze pomoże Ci "ogarnąć" RODO w Twojej organizacji?

Bądź na bieżąco :). Zapisz się na nasze media, dzięki czemu nie ominą Cię żadne nowości i zmiany w RODO przepisach. Przygotowaliśmy dla Ciebie wszystkie możliwe formy przekazywania informacji, dzięki czemu każdy będzie mógł znaleźć coś dla siebie:

- Lubisz czytać? Zapraszamy do naszego blogowego newslettera (ikonka białej koperty po lewej stronie), albo media społecznościowe: LinkedIn lub Facebook.
- Bardziej przemawia do Ciebie forma video? Zapraszamy na nasz kanał na YouTube – Czas na RODO.

- A może wolisz nas posłuchać podczas biegania / zmywania / jazdy samochodem / spaceru z psem? Zapraszamy do naszych podcastów :). Posłuchasz nas na: Spotify, Google Podcasts, SoundCloud, BuzzSprout, RSS.

A jeśli masz jakieś pytania – pisz w komentarzu – na KAŻDY odpiszemy.

Życzę Ci powodzenia we wdrażaniu RODO i ogarnianiu wszystkich 5 filarów, do zobaczenia / usłyszenia / napisania :)!

Autor artykułu:

Łukasz Zegarek

Źródła:

- Rozporządzenie 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)
- praktyczne doświadczenie budowania systemów ochrony danych osobowych od 2008 roku (jako ABI) i po 2018 roku (jako IOD).