PRZEWODNIK PO

RODO

DLA PRZEDSIĘBIORCÓW

MINISTERSTWO CYFRYZACJI
MAJ 2018


Photo by Scott Rodgerson on Unsplash

Prowadzisz jednoosobową działalność gospodarczą? Jesteś pracownikiem firmy, w której nadal nie wiecie, jak przygotować się do RODO?

JEŚLI TAK, TO TEN PRZEWODNIK JEST DLA CIEBIE.

SPIS TREŚCI:

25 MAJA 2018 ROKU

25 maja 2018 roku we wszystkich krajach należących do Unii Europejskiej zacznie być stosowane ogólne rozporządzenie o ochronie Danych osobowych 2016/679 (RODO).

RODO

obejmuje swoim zastosowaniem wszystkie podmioty – prywatne i publiczne – które przetwarzają dane osobowe i w praktyce realizują większość procesów przetwarzania danych. Regulacje RODO pomagają też wszystkim osobom przebywającym na terytorium Polski egzekwować ich prawo do ochrony danych osobowych.

Zgodnie z nowymi przepisami, dane osobowe to takie dane, które pozwalają jednoznacznie zidentyfikować osobę fizyczną. Mogą to być informacje takie jak: imię, nazwisko, numer PESEL, płeć, adres e-mail, ale również mniej oczywiste jak numer IP, dane o lokalizacji, kod genetyczny, poglądy polityczne czy historia zakupów. Wszelkie informacje zbierane na temat osoby, które pozwalają na ustalenie jej tożsamości, są danymi osobowymi, niezależnie od tego, czy są przetwarzane w formie papierowej czy cyfrowej.

W tym przewodniku opisaliśmy RODO z perspektywy różnych form działalności gospodarczej, jednakże zachęcamy do zapoznania się także z obszerniejszą publikacją, opracowaną przez Ministerstwo Przedsiębiorczości i Technologii z myślą o Małych i Średnich Przedsiębiorstwach (MŚP).

CO MUSISZ WIEDZIEĆ?

▪ NEUTRALNOŚĆ TECHNOLOGICZNA

RODO nie daje konkretnych wytycznych co do rozwiązań technologicznych, jakie należy podjąć w celu zabezpieczenia danych osobowych. Wskazując cel, jakim jest ochrona prywatności i zabezpieczenie danych osobowych, nie podaje jednego sposobu na jego osiągnięcie. Wybrana metoda technologiczna musi być przede wszystkim skuteczna. Inna będzie dobra w salonie fryzjerskim, przetwarzającym dane osobowe kilkudziesięciu klientów, a inna w sklepie internetowym, który dziennie przetwarza dane tysięcy osób.

W praktyce: realizacją art. 32, który mówi o neutralności technologicznej może okazać się rozwiązanie organizacyjne, czyli na przykład odpowiednie zabezpieczenie pomieszczenia, w którym przechowywane są dane oraz wyznaczenie osoby, odpowiedzialnej za dostęp do nich. Jeśli jednak posiadamy dane wrażliwe (np. orientacja seksualna, poglądy polityczne, stan zdrowia) i wykorzystujemy je na dużą skalę to odpowiedzią na ogromne ryzyko, związane z ich przetwarzaniem powinno być znacznie bardziej zaawansowane technologicznie zabezpieczenie.

• ZASADA MINIMALIZMU

Zbierane dane osobowe muszą być adekwatne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

W praktyce: prowadzę firmę zajmującą się tworzeniem aplikacji dostępnych za darmo do pobrania. Stworzyłem aplikację „kalkulator". Podczas instalacji aplikacja nie powinna żądać dostępu do kontaktów, zdjęć, mikrofonu czy aparatu, bowiem nie jest to niezbędne do realizacji celu aplikacji, jakim jest wykonywanie obliczeń.

Photo by NeONBRAND on Unsplash

• ZASADA ROZLICZALNOŚCI

Administrator jest odpowiedzialny za przestrzeganie przepisów o ochronie danych osobowych i musi być w stanie wykazać ich przestrzeganie.

W praktyce: jeśli moja firma zostanie skontrolowana przez organ nadzorczy pod kątem poprawności przetwarzania danych osobowych, to muszę dysponować dokumentacją potwierdzającą ich prawidłowe zabezpieczanie. Sam fakt, że nie doszło do naruszenia i nie zgłosiła się żadna poszkodowana osoba nie wystarczy za dostateczny dowód. Jako administrator muszę umieć wykazać, że dysponuję podstawą do przetwarzania danych osobowych.



• INSPEKTOR OCHRONY DANYCH (IOD)

IOD ma za zadanie monitorowanie przestrzegania obowiązków wynikających z RODO. Inspektor pełni także funkcję pośrednika pomiędzy przedsiębiorstwem a osobami, których dane są przetwarzane oraz pomiędzy przedsiębiorstwem a organem nadzorczym. Do zadań IOD będzie też należało przeprowadzenie oceny ryzyka, związanego z przetwarzaniem danych i dopasowanie do niego środków technologicznych, które je zminimalizują. Zadania IOD w szczegółach opisuje art. 39 RODO.

CZY MUSZĘ GO WYZNACZYĆ?

- Tak, jeśli przetwarzam dane osobowe na dużą skalę.
- Tak, jeśli główną moją działalnością jest przetwarzanie danych osobowych.
- Tak, jeśli prowadzę regularne i systematyczne monitorowanie (wszelkie formy śledzenia i profilowania w sieci).

• REJESTR CZYNNOŚCI PRZETWARZANIA

To dokument, w którym zapisuje się informacje o czynnościach dokonywanych na danych osobowych.

JAKĄ POWINIEN MIEĆ FORMĘ?

Może mieć zarówno formę pisemną (papierową), jak i elektroniczną. Ważne, żeby posiadał wszystkie niezbędne informacje. Format pliku, w jakim będą one przechowywane nie jest kluczowy.

CO POWINIEN ZAWIERAĆ?

Dane kontaktowe administratora i Inspektora Ochrony Danych, cele przetwarzania, opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych, informacje o odbiorcach, którym dane zostały udostępnione, planowane terminy usunięcia danych (jeśli jest to możliwe), ogólny opis środków technicznych, którymi dane są zabezpieczone

CZY MUSZĘ GO PROWADZIĆ?

Nie, jeśli prowadzę działalność gospodarczą i zatrudniam mniej niż 250 osób, chyba że przetwarzanie, którego dokonuję:

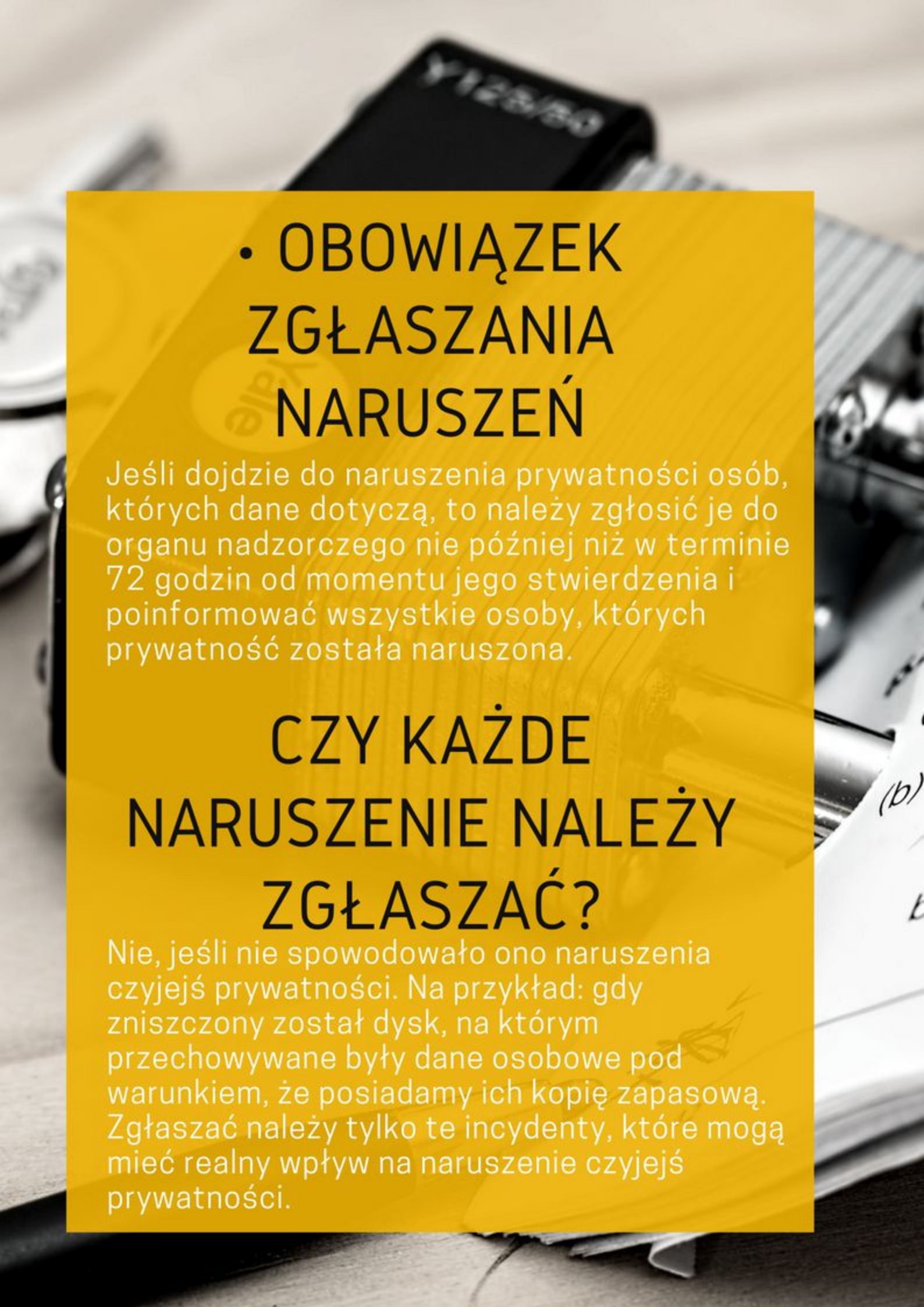
- może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub
- dane osobowe dotyczące wyroków skazujących i naruszeń prawa.

• OBOWIĄZEK INFORMACYJNY

Osoba, której dane dotyczą, musi być poinformowana o prowadzeniu operacji przetwarzania i o jego celach, a także o profilowaniu i jego konsekwencjach.

JAK SPEŁNIĆ?

Obowiązek informacyjny można realizować na wiele sposobów, na przykład:
- wysłanie osobnej wiadomości z informacją o przetwarzaniu danych osobowych,
- zamieszczanie takiej informacji w stopce każdego wysyłanego przez nas maila.



• OBOWIĄZEK ZGŁASZANIA NARUSZEŃ

Jeśli dojdzie do naruszenia prywatności osób, których dane dotyczą, to należy zgłosić je do organu nadzorczego nie później niż w terminie 72 godzin od momentu jego stwierdzenia i poinformować wszystkie osoby, których prywatność została naruszona.

CZY KAŻDE NARUSZENIE NALEŻY ZGŁASZAĆ?

Nie, jeśli nie spowodowało ono naruszenia czyjejś prywatności. Na przykład: gdy zniszczony został dysk, na którym przechowywane były dane osobowe pod warunkiem, że posiadamy ich kopię zapasową. Zgłaszać należy tylko te incydenty, które mogą mieć realny wpływ na naruszenie czyjejś prywatności.

CO WARTO ZROBIĆ?

1. Certyfikat

To nic innego jak potwierdzenie, że Twoja firma przetwarza dane osobowe w sposób poprawny i całkowicie zgodny z RODO.

Dlaczego warto? Certyfikat:

1. Wzmacnia pozytywny wizerunek firmy w oczach Twoich klientów.
2. Jest bardzo ważnym czynnikiem łagodzącym przy ewentualnym naruszeniu i postępowaniu organu nadzorczego.
3. Docelowo da Ci przewagę konkurencyjną w przetargach zamówień publicznych.

Kto je będzie wydawał?

Uprawniony do tego będzie organ nadzorczy (Prezes Urzędu Ochrony Danych Osobowych) oraz podmioty akredytowane przez Polskie Centrum Akredytacji.

Czy będzie płatny?

Tak. Opłata wyniesie czterokrotność średniej krajowej w przypadku tego wydawanego przez Prezesa Urzędu Ochrony Danych Osobowych. W przypadku podmiotów akredytowanych (przez Polskie Centrum Akredytacji) ceny mogą być inne.

2. Kodeks postępowania

To zbiór dobrych praktyk w zakresie ochrony danych osobowych w konkretnym środowisku. Nie jest obowiązkowy, ale warto go przyjąć.

Dlaczego warto?

Jest bardzo wiele charakterystycznych dla danej formy działalności gospodarczej czynności przetwarzania danych osobowych. Te czynności są powtarzalne i łatwe do zdefiniowania. Na przykład podobnych czynności na co dzień dokonywać będą mechanicy samochodowi, podobnych przedsiębiorcy prowadzący sklep internetowy czy osoby prowadzące jednoosobową działalność gospodarczą w sektorze B2B. Warto zatem wspólnie ustalić zasady postępowania w określonych sytuacjach.

Photo by Jan Kahánek on Unsplash

CZY JEGO PRZESTRZEGANIE BĘDZIE SPRAWDZANE?

Tak. Organ nadzorczy wyznaczy tak zwane podmioty monitorujące, które będą sprawdzały, czy przestrzegane są zasady zawarte w Kodeksach (tylko w przypadku przedsiębiorców, kodeksy organów publicznych nie będą monitorowane). Zatem Kodeks jest zobowiązujący, nie może mieć miejsca sytuacja stworzenia Kodeksu i nieprzestrzegania jego wytycznych.

CZY JEST PŁATNY?

Nie, jest całkowicie bezpłatny.

JAK REALIZOWAĆ PRAWA I OBOWIĄZKI WYNIKAJĄCE Z RODO

▪ PRAWO DO BYCIA ZAPOMNIANYM – CZY DZIAŁA ZAWSZE?

Nie. Przedsiębiorca będzie miał prawo odmówić realizacji żądania usunięcia danych, jeśli czyniąc to pozbawi się możliwości wyegzekwowania zobowiązań ze strony klienta lub obrony przed ewentualnymi roszczeniami.

NA PRZYKŁAD:

Prowadzę sklep internetowy sprzedający odzież. Mój klient po realizacji zamówienia zgłasza prawo do usunięcia wszystkich jego danych. Czy mogę odmówić? Tak, bowiem usuwając te dane narażam się na ewentualne roszczenia na przykład ze strony Urzędu Skarbowego albo ze strony samego klienta, który będąc nieuczciwym po realizacji zamówienia i usunięciu jego danych potwierdzających realizację zakupu może twierdzić, że do tej realizacji nie doszło i żądać zadośćuczynienia.

JAK REALIZOWAĆ PRAWA I OBOWIĄZKI WYNIKAJĄCE Z RODO

▪ PRAWO DO PRZENOSZENIA DANYCH

NA PRZYKŁAD:

Złożyłem wniosek kredytowy w Banku A. Dopełniłem wszystkich formalności, ale Bank nie wyraził zgody na udzielenie mi kredytu. Chcę zatem złożyć wniosek w Banku B. Mam w związku z tym prawo zażądać od Banku A, aby przeniósł moje dane osobowe do Banku B. Dzięki temu uniknę konieczności ponownego wypełniania tych samych formalności. Każdy przedsiębiorca będzie zobowiązany zrealizować takie żądanie.

JAK REALIZOWAĆ PRAWA I OBOWIĄZKI WYNIKAJĄCE Z RODO

▪ OBOWIĄZEK UZYSKANIA ZGODY RODZICA NA PRZETWARZANIE DANYCH DZIECKA – KIEDY NIE OBOWIĄZUJE?

W przypadku gdy przetwarzane są dane osobowe dziecka poniżej 16 roku życia istnieje obowiązek uzyskania zgody na takie przetwarzanie od rodzica.

CZY ZAWSZE?

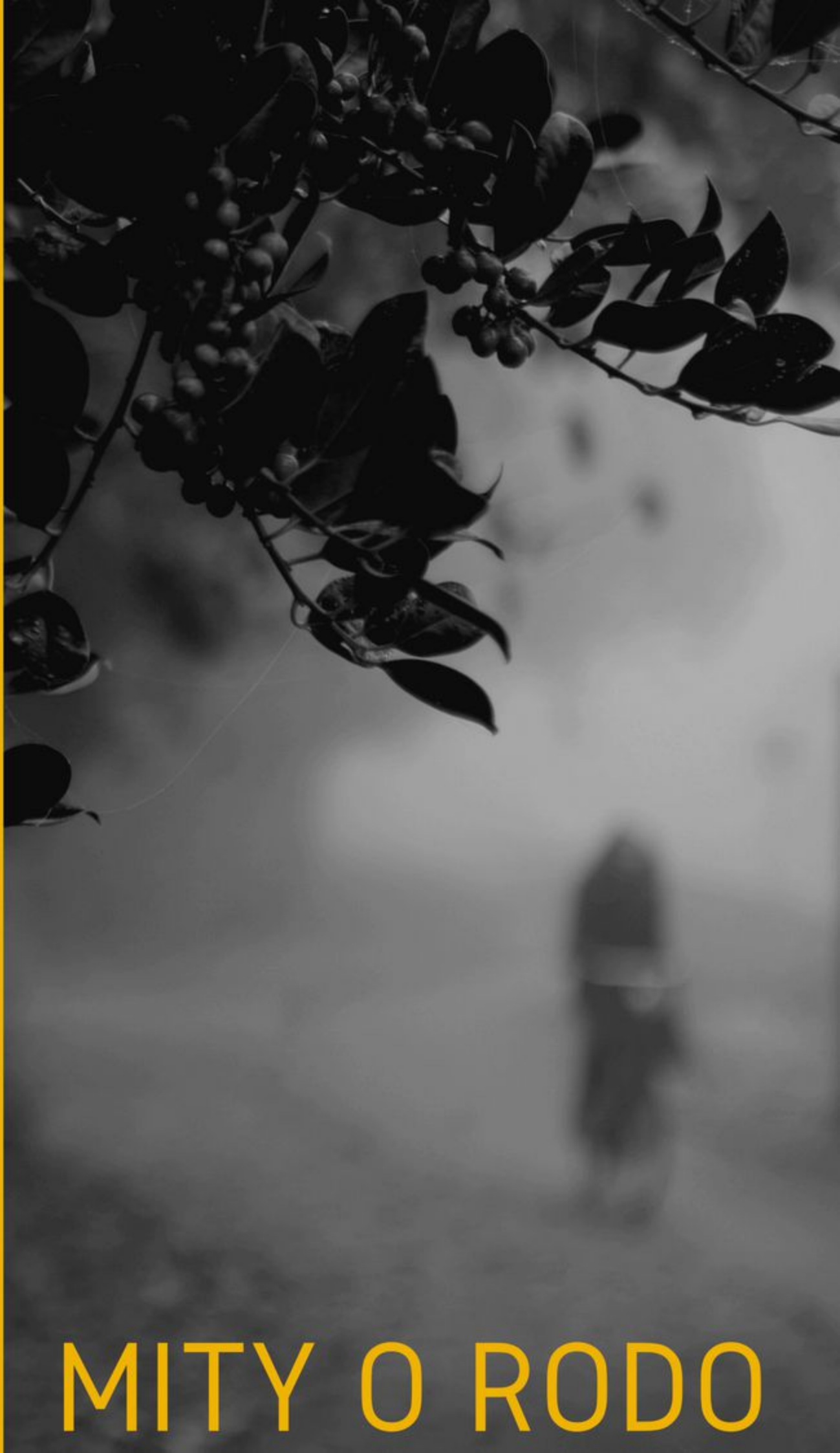
Nie. Obowiązek nie będzie obowiązywał wszędzie tam, gdzie podstawą przetwarzania będzie akceptacja regulaminu świadczenia usług drogą elektroniczną – a więc w większości przypadków.

KIEDY TAK?

Na przykład przedsiębiorca prowadzący klub tenisowy, jeśli będzie chciał umieścić zdjęcia z meczu 14-letniego Tomka z 15-letnim Michałem na stronie internetowej klubu będzie musiał uprzednio otrzymać na to zgody rodziców obu chłopców.

ZAKAZY

- NIE WYKORZYSTUJ DANYCH W CELACH MARKETINGOWYCH BEZ ZGODY OSOBY, KTÓRYCH DANE DOTYCZĄ,
- NIE UDOSTĘPNIAJ BEZ ZGODY CZYJEGOŚ WIZERUNKU,
- NIE UDOSTĘPNIAJ BEZ PODSTAWY DANYCH INNEMU PODMIOTOWI,
- NIE WYKORZYSTUJ DANYCH OSOBOWYCH KANDYDATÓW W PRZYSZŁYCH REKRUTACJACH BEZ ICH ZGODY,
- NIE GROMADŹ DANYCH W NADMIARZE, NA ZAPAS.



MITY O RODO

• PŁATNE SZKOLENIA – CZY SĄ OBOWIĄZKOWE?

Absolutnie nie. Kluczowe jest przygotowanie się do wejścia w życie nowych przepisów i poznanie obowiązków, wynikających z nowych regulacji. To, czy przedsiębiorca przygotuje się do RODO poprzez udział w płatnych szkoleniach, czy na własną rękę i bez ponoszenia kosztów zaznajomi się z unijnym rozporządzeniem, jest kwestią indywidualnej decyzji.

• APLIKACJE I PROGRAMY – CZY NAS WYRĘCZĄ?

Nie ma aplikacji i programów, które całkowicie wyręczą nas w realizacji obowiązków, wynikających z nowych przepisów. Nowe prawo wymaga od przedsiębiorców pełnego zaangażowania i stosowania się do jego zaleceń. Żaden program nie zrobi tego w 100% za nas.

• KARY FINANSOWE – CZY BĘDĄ CZĘSTE I DUŻE?

Największy mit unijnej reformy. Kary finansowe będą ostatecznością! Przed jej nałożeniem organ nadzorczy będzie miał możliwość upomnienia czy ostrzeżenia. Kary nie będą też nakładane za małe uchybienia czy niedociągnięcia. Kluczowe jest, aby każda firma wykazała zaangażowanie i świadomość w zakresie obowiązku ochrony prywatności swoich klientów i kontrahentów.

Ministerstwo
Cyfryzacji

ul. Królewska 27
00-060 Warszawa
NIP 5213621697
Regon 145881488

Projekt: Wydział Komunikacji Ministerstwa Cyfryzacji