# SZKOŁA RODO

**Wybór case’ów omawianych podczas zajęć**

Kancelaria Maruta Wachta sp. j.

MARUTA

# Kancelaria Maruta Wachta

- Kancelaria głównie znana z **IT i nowych technologii**
- Zwycięstwo w **the Lawyer 2018** oraz w rankingu Rzeczpospolita



# Zespół RODO

30 prawników oraz eksperci techniczni i biznesowi

– prawdopodobnie największy taki zespół w Polsce

Nagroda Rzeczpospolitej 2018

– Lider w dziedzinie ochrony danych

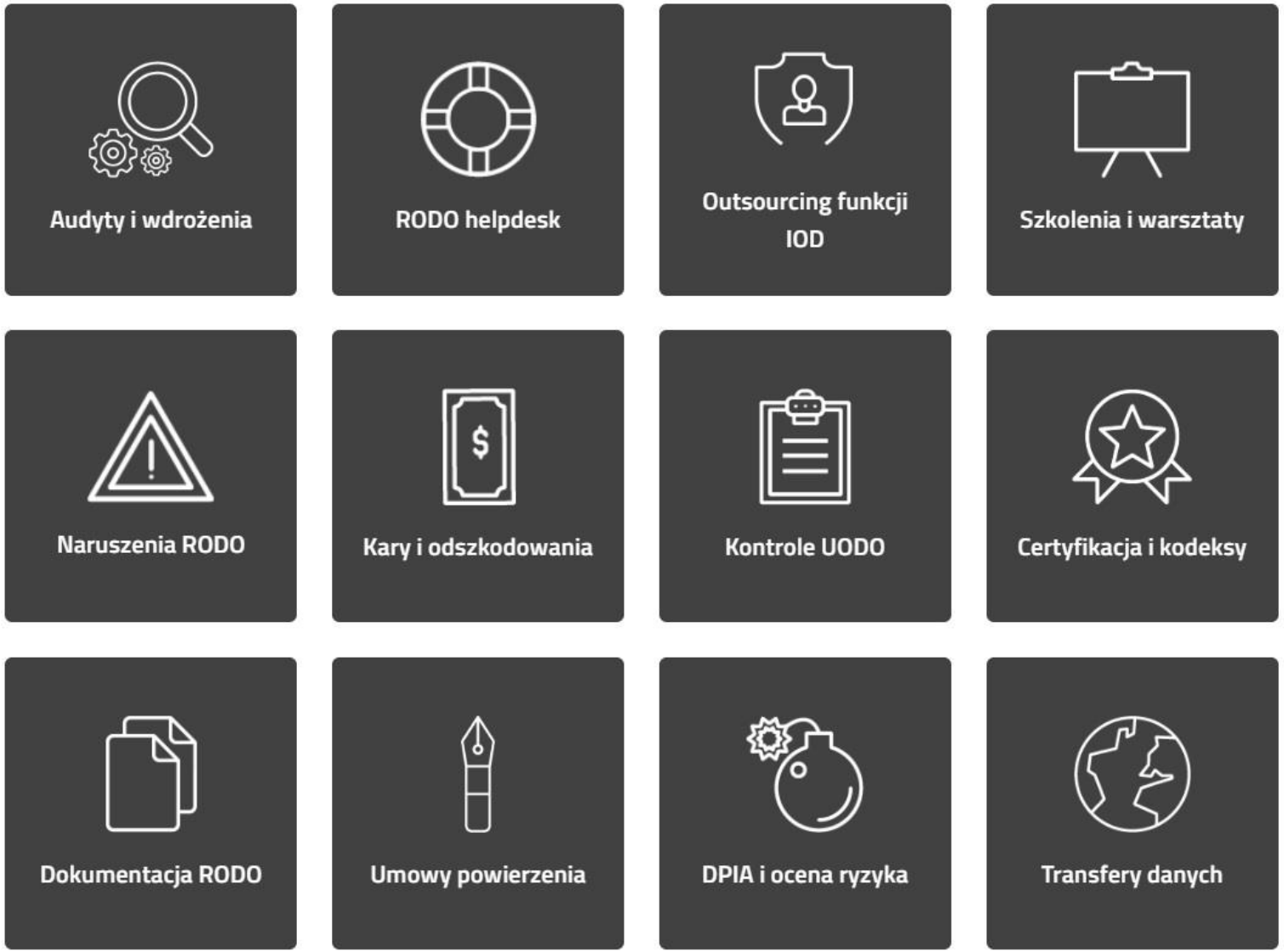
W zakresie RODO pomogliśmy ponad 100

organizacjom publicznym i prywatnym ze wszystkich dziedzin gospodarki

# Usługi RODO

## SPECJALIZACJE

- IT i nowe technologie
- Telekomunikacja
- Sektor finansowy
- Energetyka
- e-commerce
- e-marketing
- Sieci handlowe i franczyzowe
- Sektor publiczny
- HR
- Branża produkcyjna

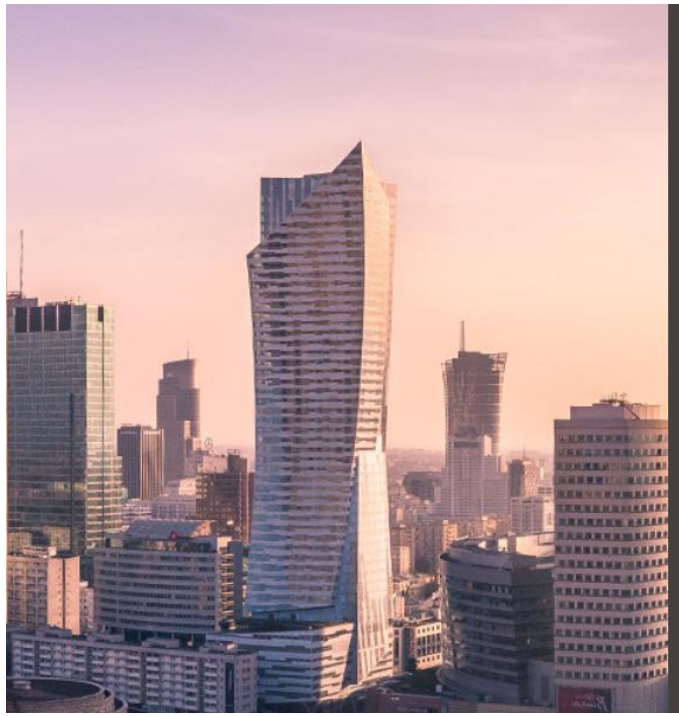


# Napisz do nas

**kontakt_rodo@maruta.pl**

Newsletter

**newsletter_rodo@maruta.pl**



## Dane kontaktowe

Warszawa

ul. Wspólna 62
00-684 Warszawa
Ufficio Primo

biuro@maruta.pl
+48 22 128 00 00
+48 22 32 32 321

# PRAKTYCZNE PODSTAWY RODO

# Case 1

**Spółka X zleciła domowi mediowemu zrealizowanie kampanii marketingowej** w postaci wysyłki newslettera do kobiet w wieku 18-25 lat, mieszkających w Warszawie. Spółka X zapewniła sobie umownie możliwość weryfikacji osób, do których przesyłany jest mailing, jednak nie ma bieżącego dostępu do bazy danych tworzonej przez dom mediowy. Dom mediowy zamierza w przyszłości wykorzystywać zgromadzone leady w celu świadczenia usług dla innych klientów.

**Czy Spółka X powinna zawrzeć z domem mediowym umowę powierzenia?**

# Case 2

**Kamera zainstalowana w korytarzu i recepcji spółki X zapisuje nagranie ruchu w korytarzu.** Nagrania zawierają wizerunki przechodzących korytarzem osób. Celem monitoringu korytarza jest zapewnienie bezpieczeństwa mienia i osób. Nagrania są przechowywane przez 6 miesięcy.

Początkujący nerd ochrony prywatności (od niedawna w firmie) zwrócił uwagę, że dane z nagrań mogą zdradzać pochodzenie etniczne i należy monitoring wyłączyć.

**Wczuj się w sytuację wiceprezesa odpowiedzialnego za Compliance i odpowiedz na argumenty pracownika. Znajdź inny błąd spółki X.**


# UMOWY POWIERZENIA PRZETWARZANIA DANYCH

# Case 1

**Zamawiający usługi IT**, chcąc zabezpieczyć się na wypadek sytuacji, gdy konkretne zadanie wymagałoby **szerszego niż z reguły dostępu do danych**, proponuje dostawcy Smart Data zawarcie w umowie powierzenia następującego postanowienia:

**Zakres powierzenia wskazany w Załączniku do niniejszej Umowy może zostać zmieniony (rozszerzony lub ograniczony) przez Administratora w dowolnym momencie poprzez złożenie procesorowi stosownego oświadczenia w formie pisemnej pod rygorem nieważności.**

**Smart Data obawia się**, że powyższe postanowienie otwiera drogę do manipulowania przedmiotem umowy i zlecania zadań nieprzewidzianych pierwotnie w umowie.

# Case 2

**Spółka Szyj i Żyj świadczy usługi luksusowego krawiectwa**, co wymaga gromadzenia danych klientów (np. ich wymiarów, upodobań odzieżowych itp.). Dane te przechowywane są przez Super Dane sp. z o.o. zajmujące się hostingiem. W umowie o świadczenie usług wskazano jedynie, że:

**Super Dane zobowiązuje się przechowywać dane na serwerach opisanych w załączniku nr 1, z zastosowaniem zabezpieczeń określonych w załączniku 2. Po zakończeniu umowy Super Dane zobowiązuje się zwrócić wszystkie dane Zamawiającemu.**

Umowa powierzenia zawiera wyłącznie standardowe postanowienia wynikające z RODO. **Do Spółki Szyj i Żyj zgłosił się klient żądający „zapomnienia danych”** – żądanie okazało się częściowo skuteczne. Szyj i Żyj nakazało więc spółce Super Dane przeniesienie danych ze środowiska produkcyjnego do archiwalnego (przeznaczonego na ewentualne dochodzenie roszczeń). Wykonawca żąda jednak za takie działania dodatkowego wynagrodzenia.

# OBSŁUGA ŻĄDAŃ PODMIOTÓW DANYCH

# Case 1

**Spółka CzytajMY prowadzi działalność wydawniczą oraz e-commerce.** W celu założenia konta w jej serwisie internetowym niezbędne jest podanie adresu e-mail oraz wygenerowanie hasła. Na koncie gromadzone są informacje o historii zakupów i szczegóły dotyczące karty płatniczej (jeśli klient z niej korzysta).

Do Spółki wpłynęło żądanie o następującej treści: „Proszę o usunięcie mojego konta – zakładałam je mniej więcej w marcu 2016 roku, na adres malaLadyPank@tlen.pl”.

Mail został przesłany z adresu: MyFairLady@tlen.pl

**W jaki sposób CzytajMy może zweryfikować tożsamość wnioskodawcy?**

# Case 2

**Spółka Tort S.A. prowadzi portal, na którym zarejestrowani klienci mogą oceniać i recenzować cukiernie prowadzące działalność w Polsce.** W ramach rejestracji w portalu zbierane są informacje: imię, nazwisko, adres zamieszkania.

Tort S.A., podczas korzystania przez użytkowników z portalu oraz aplikacji na urządzenia mobilne, zbiera informacje o odwiedzonych miejscach, godzinach logowania, wystawionej ocenie lokali. Tort S.A. stosuje w portalu pliki cookies, zbierające informacje o urządzeniach użytkowników.

Użytkownik Jan Skrzetuski złożył do Tort S.A. wniosek o kopię danych.

**Jak powinna wyglądać odpowiedź? Jakie informacje powinna zawierać?**


# KLAUZULE INFORMACYJNE I ZGODY

# Case 1

**Robert B. zainteresowany zawarciem umowy o prowadzenie rachunku oszczędnościowego** odwiedził oddział Banku Pełna Sakiewka z siedzibą w Warszawie przy ul. Bogatej 5. Po zapoznaniu się z ofertą Banku zdecydował się na założenie konta. Pracownik wprowadził do systemu dane osobowe z dowodu osobistego Roberta B. i przystąpił do przygotowania umowy, którą następnie Robert B. podpisał.

W ramach prowadzonej działalności Bank współpracuje z firmą świadczącą na jego rzecz usługę IT oraz druku i wysyłki korespondencji. Bank powołał Inspektora Ochrony Danych Osobowych.

**Jakie informacje dot. procesu przetwarzania danych osobowych Bank powinien przekazać Robertowi B. i w jakim czasie?**

# Case 2

**Man Sp. z o.o. przydziela kilku swoim pracownikom samochody służbowe.**
W związku z tym ich dane osobowe przetwarza w następujących celach:

a) przydzielenia samochodów służbowych,
b) wypełniania przez administratora danych obowiązków nałożonych przez obowiązujące przepisy, w tym rozliczenia kosztów jego eksploatacji,
c) obsługi wezwań kierowanych do administratora przez organy właściwe w sprawie popełnienia wykroczeń drogowych,
d) obsługi awarii i szkód powstałych w trakcie korzystania z pojazdu,
e) podejmowania ewentualnych czynności w związku z przeciwdziałaniem przestępstwom przeciwko administratorowi danych,
f) dochodzenia ewentualnych roszczeń lub obrony przed ewentualnymi roszczeniami.

**Proszę sformułować obowiązek informacyjny w zakresie celów i podstaw prawnych przetwarzania.**

# NARUSZENIE OCHRONY DANYCH OSOBOWYCH

# Case 1

**Do hotelu zwrócił się mężczyzna.** Powołując się na okazaną odznakę policyjną, zwrócił się o udostępnienie mu zapisu z monitoringu wizyjnego przy recepcji hotelu, wskazując na konkretną datę i godzinę. Hotel wnioskowany zapis udostępnił.

Mężczyzna okazał się nie być policjantem, a pozyskane materiały wykorzystał przeciwko żonie w sprawie rozwodowej. Jej wizerunek oraz wizerunek innego mężczyzny, w którego towarzystwie była ta kobieta, był wyraźnie widoczny na przekazanym zapisie. Na zapisie widoczne były także wizerunki innych gości hotelu.

**Czy mamy do czynienia z naruszeniem?**
**Czy występuje ryzyko naruszenia praw i wolności? Jakie ryzyko?**
**Jakie skutki może wywołać naruszenie?**

# Case 2

**W wyniku wypadku komunikacyjnego** bus przewożący archiwalną dokumentację bankową do zniszczenia przewrócił się na jezdni.

W wyniku zdarzenia wysypały się na jezdnię niezabezpieczone dokumenty zawierające dane osobowe. Usługi transportu i niszczenia dokumentów dla banku świadczyła ta sama firma zewnętrzna.

**Jak powinien zachować się procesor?**
**Od kiedy jest liczony moment stwierdzenia naruszenia?**
**Czy należy zawiadomić osoby, których dane dotyczą?**

# PROWADZENIE REJESTRÓW W PRAKTYCE

# Case 1

**Spółka Little Dream przeprowadza inwentaryzację swoich procesów przetwarzania danych**, na podstawie której sporządzi rejestr czynności przetwarzania. Dział HR spółki przygotował następujący opis wykonywanych przez siebie operacji przetwarzania: „zbieranie informacji o kandydatach do pracy na podstawie CV nadesłanych w odpowiedzi na ogłoszenie o pracę, wstępna selekcja CV, wybór kandydatów, którzy zostaną zaproszeni na rozmowy rekrutacyjne, przeprowadzenie rozmów rekrutacyjnych, podczas których mogą zostać zebrane dodatkowe informacje o kandydatach,  ocena kandydatów oraz wybór kandydata do pracy, zatrudnienie kandydata wybranego w wyniku przeprowadzonej rekrutacji”.

**Jakie czynności przetwarzania należy wpisać w rejestrze czynności na podstawie opisu przygotowanego przez dział HR Spółki?**

# Case 2

Zgodnie z ustawą o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu **bank Zysk SA jest zobowiązany do przekazywania do Generalnego Inspektora Informacji Finansowej** informacji o przyjętej wpłacie lub dokonanej wypłacie środków pieniężnych o równowartości przekraczającej 15 000 euro (przekazywane informacje obejmują dane identyfikacyjne klientów banku). Ponadto, bank ma obowiązek zawiadamiać Generalnego Inspektora o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu – w zawiadomieniu należy wskazać m.in. dane identyfikacyjne klientów banku, których dotyczy zawiadomienie.

**Czy Generalny Inspektor Informacji Finansowej powinien być uwzględniony w rejestrze czynności przetwarzania jako odbiorca danych klientów banku? Proszę uzasadnić swoje stanowisko.**

# HR ORAZ INNA DZIAŁALNOŚĆ PODSTAWOWA

# Case 1

**Spółka Misty Blue zleciła agencji rekrutacyjnej Jack & James rekrutację na stanowisko dyrektora zarządzającego.** W zleceniu Misty Blue zastrzegła jednak, że rekrutacja ma mieć charakter ukryty oraz agencja nie może ujawnić tożsamości Misty Blue kandydatom.

Agencja ma przesłać do Misty Blue CV pięciu najlepszych kandydatów, z których Misty Blue wybierze dwóch i zaprosi ich na rozmowę. Wraz z zaproszeniem Misty Blue prześle do dwóch najlepszych kandydatów klauzule informacyjne.

**Czy prowadzenie rekrutacji ukrytej jest w świetle RODO dopuszczalne?**

# Case 2

**Spółka Misty Blue w regulaminie pracy wskazała, że zakazane jest korzystanie przez pracowników ze służbowej poczty elektronicznej w celach prywatnych.** Pracownicy zostali poinformowani, że pracodawca może prowadzić monitoring poczty służbowej. W dniu 16 sierpnia 2018 r. spółka stwierdziła, że doszło do wycieku poufnych informacji, do których dostęp miało ograniczone grono osób, w tym Jan Kowalski. Spółka przeszukała służbową skrzynkę Jana Kowalskiego oraz ustaliła, że był on źródłem wycieku poufnych informacji. Jan Kowalki złożył pozew przeciwko Misty Blue zarzucając spółce naruszenie tajemnicy korespondencji oraz naruszenie jego prawa do prywatności.

**Czy zarzuty Jana Kowalskiego są słuszne?**

# MARKETING, MEDIA SPOŁECZNOŚCIOWE, TRANSFERY DANYCH

# Case 1

**Spółka produkująca soczewki kontaktowe postanowiła przeprowadzić konkurs.** W konkursie może wziąć udział każdy. Aby wziąć udział w konkursie, należy polubić post konkursowy, a w komentarzu napisać odpowiedź na pytanie: „Jak zniewalasz spojrzeniem?”. Nagrodami w konkursie jest 10 maskotek bazyliszka.

Tworząc klauzulę informacyjną, eksperci spółki nabrali wątpliwości, jaka będzie podstawa prawna przetwarzania danych uczestników konkursu. Rozważane warianty to zgoda, niezbędność do wykonania umowy oraz uzasadniony interes.

**Jaka jest podstawa przetwarzania danych osobowych na potrzeby konkursu? Przygotuj klauzulę informacyjną.**

# Case 2

**Spółka A postanowiła rozpocząć program lojalnościowy.** Spółka chciałaby wykorzystać program do budowania bazy kontaktów w celu marketingowym oraz w oparciu o zgromadzone informacje lepiej dopasowywać przekaz marketingowy do indywidualnych klientów. Klienci będący członkami programu będą otrzymywać dedykowane rabaty. Otrzymają także jednorazowy bon w wysokości 50 zł na zakupy w sklepie internetowym spółki A.

**Zaproponuj formalnie poprawny model funkcjonowania takiego programu lojalnościowego. Rozważ podstawy prawne, interes biznesowy spółki A oraz inne obowiązki spoczywające na spółce A.**

# PRIVACY BY DESIGN, PREEWALUACJA I OCENA SKUTKÓW PRZETWARZANIA

# Case 1 cz. 1

**Proszę przeprowadzić ocenę ryzyka dla poniższego procesu: Świadczenie usługi „Inteligentna lodówka”.**

**Producent lodówek – firma SzronPol sp. z o.o. – postanowiła wprowadzić do obrotu supernowoczesne, wielofunkcyjne lodówki.** Lodówki firmy SzronPol wyposażone mają być w specjalne oprogramowanie dostarczane przez zewnętrzny podmiot. Oprogramowanie ma pozwalać na gromadzenie wielu informacji na specjalnej platformie (która została przygotowana przez innego dostawcę IT), gdzie każdy użytkownik ma mieć swoje własne konto. W ramach konta użytkownik będzie mógł m.in. sprawdzać kaloryczność produktów znajdujących się w lodówce; weryfikować, czy jego dieta jest odpowiednio zbilansowana; uzyskać informację o zbliżającym się upływie daty ważności określonych produktów; prowadzić bilans wydatków przeznaczanych na jedzenie.

# Case 1 cz. 2

**Lodówka ma być również połączona z systemami informatycznymi największych sieci spożywczych i pozwalać na automatyczne zamawianie produktów**, które się kończą. Dodatkową funkcjonalnością lodówki ma być możliwość badania tętna i ciśnienia krwi dzięki czujnikom umieszczonym w uchwycie. Wszystkie dane mają być automatycznie wysyłane do centralnego systemu. Tam dane mają być zestawiane z informacjami o spożywanych produktach i oceniane ma być prawdopodobieństwo zachorowania na określone choroby. Jeżeli będzie ono wysokie, dane będą wysyłane do placówki medycznej. Użytkownik będzie mógł wyłączyć tę funkcję poprzez odpowiednie ustawienia w ramach swojego konta.

SzronPol ma mieć dostęp do wszystkich danych, które będą gromadzone na platformie, będzie też decydować, w jaki sposób będą one wykorzystywane. Wszystkie dane (w tym informacje o potencjalnych chorobach) chce wykorzystywać w celach analitycznych.

# Case 1 cz. 3

**Platforma ma wykorzystywać rozwiązania chmurowe** – serwery, które będą przez nią używane, znajdują się w USA, Kanadzie oraz Indiach. Dostawca oprogramowania do lodówek będzie świadczyć na rzecz SzronPol usługi serwisowe, w ramach których uzyska dostęp do danych użytkowników.

Zarząd SzronPol dowiedział się o wysokich karach finansowych, które mogą być nakładane na gruncie RODO. Zamówił więc ekspertyzę prawną w celu weryfikacji legalności planowanych działań. Ponieważ SzronPol do tej pory sprzedawał wyłącznie standardowe lodówki, w firmie nie zostały wdrożone żadne fizyczne ani techniczne środki ochrony systemów informatycznych. SzronPol przeszedł jednak audyt prawny zgodności z RODO i ma wszelkie procedury wymagane przez przepisy.

# Case Study

**Szkoła RODO – edycja jesienna**
**już w listopadzie!** Szczegóły wkrótce.

Chcesz znać szczegóły przed innymi?
Napisz do nas na
**newsletter_rodo@maruta.pl**

Chcesz dostać pełne wersje materiałów?
Zapisz się na newsletter.

Newsletter

**newsletter_rodo@maruta.pl**

MARUTA