JDP
Drapała &
Partners

GLOBALNY COMPLIANCE, LOKALNE RYZYKA

8 Hot Spots prywatności do uwzględnienia w Polsce

Poniżej omawiamy polskie przepisy o ochronie danych osobowych oraz częste błędy popełniane przez organizacje posiadające biura w Polsce, gdzie konkretne rozwiązania wprowadzane są przez centralę za granicą. Wskazujemy potencjalne konsekwencje oraz jak można im zapobiec, wprowadzając odpowiednie narzędzia.

SPIS TREŚCI:

1. COOKIES I INNE TECHNOLOGIE ŚLEDZĄCE

POLSKA SPECYFIKA

W Polsce korzystanie z plików cookies oraz innych technologii śledzących jest ściśle regulowane przez Prawo komunikacji elektronicznej (art. 399-400 PKE). Zgodnie z tymi przepisami, pliki cookies mogą zostać umieszczone na urządzeniu końcowym użytkownika wyłącznie po uzyskaniu jego uprzedniej, aktywnej i jednoznacznej zgody. Użytkownik musi mieć możliwość wyrażenia zgody na różne kategorie plików (np. niezbędne do działania serwisu, analityczne, marketingowe) w sposób oddzielny, a także łatwo cofnąć swoją zgodę w każdym momencie. Przepisy wymagają prowadzenia czytelnego rejestru udzielonych zgód, w którym odnotowywane są informacje o tym, kto, kiedy i na co wyraził zgodę, oraz precyzują maksymalne okresy przechowywania poszczególnych rodzajów danych. Organ nadzorczy (UKE lub UODO) w trakcie kontroli sprawdza między innymi, czy baner zgody umożliwia odrzucenie wszystkich plików oraz czy logi faktycznie archiwizują historię zgód w sposób gwarantujący pełną audytowalność.

TYPOWY BŁĄD

Globalny baner soft opt-in – jeden przycisk „Akceptuj wszystko", brak opcji rezygnacji lub wyłączenia analityki. Zgoda uznawana „przez dalsze przeglądanie", brak rejestru zgód i tabel retencji.

POTENCJALNE KONSEKWENCJE BŁĘDU

- Kara Prezesa UKE – do 3% przychodu osiągniętego w Polsce.
- Kara UODO/RODO – do 20 mln EUR lub 4% globalnego obrotu.
- Nakaz natychmiastowego wyłączenia skryptów może spowodować spadek konwersji i utratę danych analitycznych.

NASZA PROPOZYCJA – WARTOŚĆ DLA KLIENTA

Co dostarcza kancelaria	Wymierna korzyść
Polityka cookies PL/EN + Baner zgody PL/EN („Akceptuję / Odrzucam / Ustawienia")	Spójny, gotowy do przyjęcia dokument; łatwe wdrożenie przez dowolny zespół web-deweloperski. Zachowanie spójnego UX grupy przy pełnej zgodności z polskimi wymogami.
Checklisty kwartalnego przeglądu zgodności	Samodzielna weryfikacja przez zespół marketingowy — ogranicza konieczność kolejnych audytów zewnętrznych i wcześniej wykrywa niezgodności.
Rejestr zgód + matryca retencji	Gotowy dowód rozliczalności do okazania UKE/UODO; uproszczenie sprawozdawczości wewnętrznej.
Warsztat „Legalne tagi w 90 minut" dla marketingu i IT	Zespół potrafi samodzielnie utrzymywać zgodność przy kolejnych kampaniach, co skraca czas „time-to-market" i zmniejsza koszty obsługi prawnej.

2. KOMUNIKACJA MARKETINGOWA (E-MAIL, SMS, PUSH, KOMUNIKATORY)

POLSKA SPECYFIKA

Każda wiadomość o charakterze handlowym — nawet wysłana na adres firmowy — wymaga wcześniejszej wyraźnej zgody odbiorcy (art. 398 PKE).

Zgoda musi być:

- odrębna od akceptacji regulaminu lub polityki prywatności,
- jednoznacznie udokumentowana (data, godzina, źródło),
- łatwa do wycofania, a organizacja ma obowiązek uszanować rezygnację w ciągu 48 h,
- odrębna na każdy kanał komunikacji np. SMS, push, e-mail, rozmowa telefoniczna).

TYPOWY BŁĄD

Masowa wysyłka „cold mailing" B2B w oparciu o „uzasadniony interes" lub jeden zbiorczy checkbox łączący zgodę marketingową. Brak centralnego dziennika zgód i historii wypisów.

POTENCJALNE KONSEKWENCJE BŁĘDU

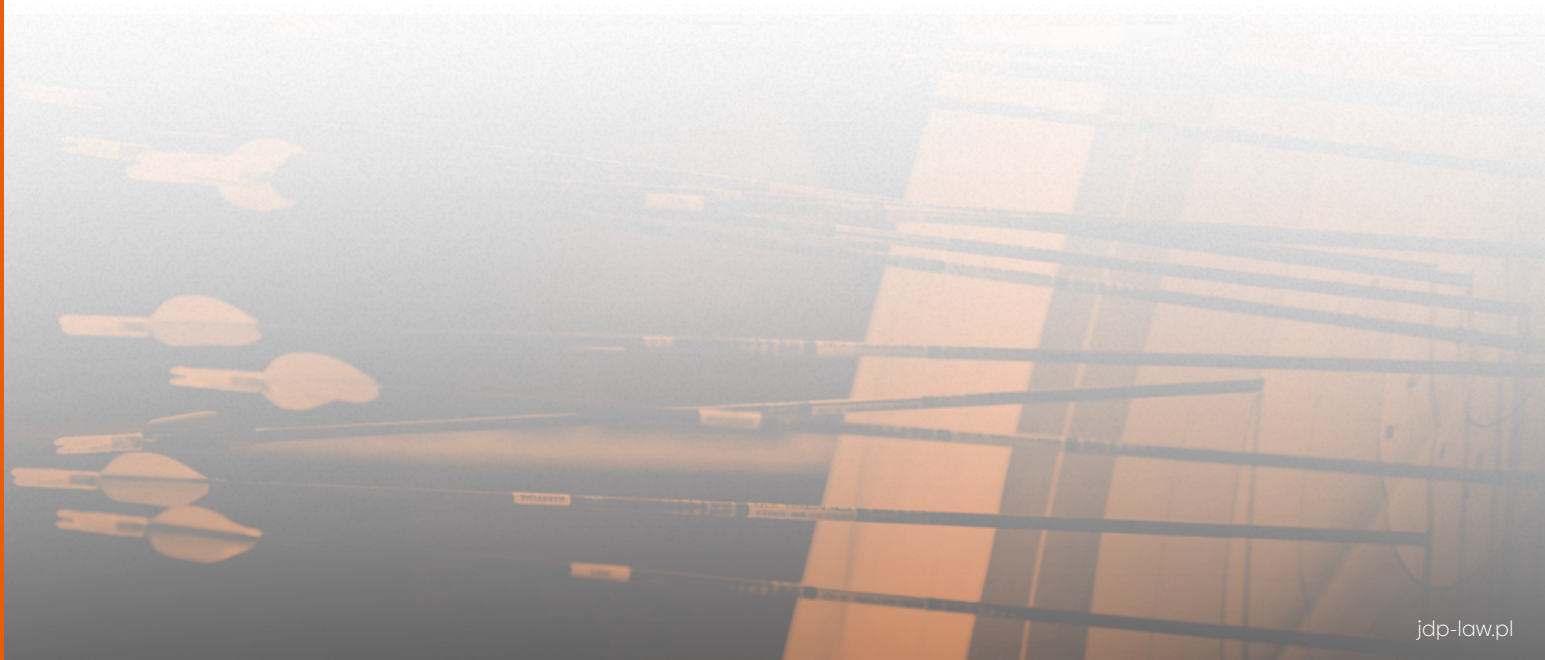
- Kara Prezesa UKE — do 3% rocznego przychodu osiąganego w Polsce.
- Kara Prezesa UOKIK dla osoby zarządzającej za umyślne działanie nawet do 2 mln zł.

Przykłady rynkowe:

- Operator telekomunikacyjny – 9,1 mln zł kary za wysłanie ponad 3,8 mln SMS-ów marketingowych bez wymaganych zgód klientów;
- 80 tys. zł kary za wykonanie ponad 30 tys. połączeń telefonicznych o charakterze marketingowym bez zgody odbiorców;
- Operator telekomunikacyjny – 2,85 mln zł kary (2024) za połączenia telefoniczne oraz wysyłanie treści marketingowych przez SMS i e-mail bez wymaganych zgód;
- Operator telekomunikacyjny – 5 mln zł kary za prowadzenie marketingu bezpośredniego z użyciem automatycznych systemów wywołujących (SMS-y reklamowe) bez zgód odbiorców, nawet gdy działania zlecono firmie zewnętrznej.

NASZA PROPOZYCJA – WARTOŚĆ DLA KLIENTA

Co dostarcza kancelaria	Wymierna korzyść
Polityka pozyskiwania zgód + makieta „centrum preferencji" (PL/EN, gotowa do wdrożenia)	Jednolity, zgodny z prawem formularz z odrębnymi checkboxami; użytkownik widzi jasne wybory, co podnosi współczynnik konwersji i minimalizuje ryzyko naruszeń PKE.
Wzorcowy rejestr zgód wraz z instrukcją integracji z dowolnym CRM	Każda zgoda ma datę, źródło i zakres — w razie kontroli UKE/UODO dział prawny eksportuje raport jednym kliknięciem.
Procedura obsługi wypisu („opt-out SLA 48 h") – instrukcja dla marketingu i IT + gotowy e-mail potwierdzający rezygnację	Szybkie usunięcie adresu z listy redukuje skargi, chroni reputację domeny i ogranicza ryzyko wysokiej kary administracyjnej.
Jednostronicowa check-lista przed kampanią (do podpisu przez właściciela kampanii)	Samokontrola zespołu marketingowego zmniejsza potrzebę stałego nadzoru prawnego, przyspiesza uruchamianie nowych wysyłek.
Mini-szkolenie online „Opt-in w 30 minut" (nagranie + materiał PDF)	Nowi pracownicy szybko rozumieją zasady, co zapewnia ciągłą zgodność bez dodatkowych kosztów onboardingowych.



3. MONITORING PRACOWNIKÓW I ODWIEDZAJĄCYCH (CCTV I POCZTA E-MAIL)

POLSKA SPECYFIKA

Każda forma monitoringu w miejscu pracy – w tym rejestracja obrazu przy użyciu kamer CCTV, śledzenie lokalizacji za pomocą GPS oraz kontrola służbowej poczty e-mail – musi być formalnie uwzględniona w regulaminie pracy zgodnie z art. 22² Kodeksu pracy. Pracodawca zobowiązany jest poinformować pracowników o planowanym wdrożeniu monitoringu z co najmniej 14-dniowym wyprzedzeniem oraz umieścić stosowne oznaczenia w rejonach objętych monitoringiem. Cel stosowania monitoringu musi być jasno określony (np. zapewnienie bezpieczeństwa, ochrona mienia, zachowanie poufności informacji), a wszelkie działania muszą być proporcjonalne do zamierzonego celu i zgodne z przepisami o ochronie danych osobowych.

TYPOWY BŁĄD

Narzędzia do skanowania poczty stosowane centralnie w grupie kapitałowej, bez rozważenia lokalnego otoczenia prawego dla tych technologii.
Odczytywanie poczty pracownika bez jego zgody poprzez dział IT, bez wdrożenia monitoringu.
System CCTV bez jasnych oznaczeń.
GPS w samochodach bez ograniczenia wykorzystania.
Monitoring telefonów służbowych bez jasnych informacji.

POTENCJALNE KONSEKWENCJE BŁĘDU

- Grzywna PIP — do 50 tys. zł;
- Kara UODO (np. 160 tys. EUR za ukryty monitoring placówki medycznej);
- Roszczenia odszkodowawcze pracowników za naruszenie dóbr osobistych lub prywatności;
- Konieczność rozważenia stosowania dowodów z nielegalnego monitoringu w sporze sądowym z pracownikiem pod kątem skutków ich wykorzystania;
- Możliwe są także sankcje karne: grzywna, ograniczenie wolności, a nawet pozbawienie wolności do 2 lat (art. 267 § 3 Kodeksu karnego).

NASZA PROPOZYCJA – WARTOŚĆ DLA KLIENTA

Co dostarcza kancelaria	Wymierna korzyść
Ocena DPIA i aktualizacja Regulaminu Pracy (CCTV + e-mail)	Monitoring zostaje uregulowany zgodnie z polskim prawem — dowody będą ważne w razie sporu bez ryzyka roszczeń regresowych.
Wzory znaków, klauzul i harmonogram kasowania nagrań	Pracownik jest prawidłowo poinformowany, co zmniejsza ryzyko skarg do PIP i UODO.
Protokół dostępu do skrzynek e-mail	HR/Legal mają jasną, zatwierdzoną procedurę — unika się zarzutów „nieuprawnionej inwigilacji".

4. PRYWATNE URZĄDZENIA I KOMUNIKATORY (BYOD)

POLSKA SPECYFIKA

W polskim środowisku prawnym pracodawca może zezwolić na przetwarzanie danych służbowych na prywatnych urządzeniach pracowników wyłącznie po uzyskaniu od nich pisemnej zgody i przeprowadzeniu odpowiedniej oceny ryzyka, uwzględniającej wymagania RODO oraz art. 22[1] Kodeksu pracy. Konieczne jest także wdrożenie rozwiązań MDM (Mobile Device Management) lub innych mechanizmów zabezpieczających urządzenia prywatne, a w procedurze zakończenia współpracy muszą być uregulowane zasady odzyskiwania lub usuwania danych firmowych znajdujących się na tych urządzeniach.

TYPOWY BŁĄD

Pracownicy korzystają z prywatnych telefonów i komputerów do celów służbowych (BYOD), ale firma nie ma żadnych ustalonych zasad ani pisemnej zgody na takie rozwiązanie (brak MDM). Urządzenia te nie są odpowiednio zabezpieczone, a w przypadku odejścia pracownika nie ma procedury odzyskania przechowywanych na nich danych firmowych.

POTENCJALNE KONSEKWENCJE BŁĘDU

- Kara RODO 4% globalnego obrotu.
- Możliwa odpowiedzialność karna kadry zarządzającej (art. 107 ustawy o ODO) za udostępnienie danych osobom nieuprawnionym.
- Utrata kontroli nad tajemnicą przedsiębiorstwa (np. baza klientów na prywatnym dysku).

NASZA PROPOZYCJA – WARTOŚĆ DLA KLIENTA

Co dostarcza kancelaria	Wymierna korzyść
Polityka BYOD i komunikatorów + wzory zgód	Pracownicy i menedżerowie mają jasne zasady, co minimalizuje ryzyko wycieku danych.
Lista wymagań MDM / szyfrowania + playbook „zgubiony telefon”	Incydent mobilny jest szybko opanowany, co może uchronić przed zgłoszeniem do UODO i karą.
Warsztat „Secure Messaging”	Zespół handlowy i obsługi klienta używa komunikatorów w sposób zgodny z prawem i wymogami branżowymi.

5. SYGNALIŚCI (WHISTLEBLOWING)

POLSKA SPECYFIKA

Polska ustawa o ochronie osób zgłaszających naruszenia prawa (tzw. whistleblowing) z 2024 r. nakłada obowiązek, by wszystkie zgłoszenia sygnalistów były przyjmowane i rozpatrywane przez dedykowaną jednostkę funkcjonującą na terytorium Polski. Organizacja musi zapewnić odpowiednie zabezpieczenia organizacyjno-techniczne, a w przypadku korzystania z zewnętrznej platformy SaaS powinna zawrzeć dodatkowe umowy gwarantujące przetwarzanie zgłoszeń zgodnie z polskimi przepisami oraz terminowe udzielanie informacji zwrotnej zgłaszającemu.

TYPOWY BŁĄD

Kanał sygnalistyczny obsługiwany wyłącznie w centrali (np. Niemcy), bez lokalnej procedury, bez polskiego zespołu decyzyjnego i bez terminowego feedbacku.

POTENCJALNE KONSEKWENCJE BŁĘDU

- Grzywna administracyjna do 50 tys. zł za brak procedury lub jej nieprawidłowe działanie.
- Odpowiedzialność karna (grzywna, ograniczenie wolności, do 3 lat pozbawienia wolności) za działania odwetowe.
- Wizerunkowy kryzys po ujawnieniu sprawy mediom lub organom zewnętrznym.

NASZA PROPOZYCJA – WARTOŚĆ DLA KLIENTA

Co dostarcza kancelaria	Wymierna korzyść
Lokalizacja globalnego kanału (DPIA, procedura PL, rejestr zgłoszeń)	Firma spełnia wymogi ustawy bez konieczności wymiany całej platformy IT.
Szkolenie komisji ds. zgłoszeń	Decyzje zapadają szybko i zgodnie z prawem, co minimalizuje ryzyka karne i reputacyjne.
„Dry-run" – test incydentu	Zespół zna procedurę w praktyce, a luki naprawia się przed realnym zgłoszeniem.

6. POLITYKI OCHRONY DANYCH I IMIENNE UPOWAŻNIENIA

POLSKA SPECYFIKA

Organ nadzorczy (UODO) w swoich decyzjach wielokrotnie podkreśla, że każdy pracownik musi posiadać imienne upoważnienie do przetwarzania danych osobowych, zawierające zakres czynności oraz systemy, do których przetwarzania jest uprawniony. Polityka ochrony danych powinna odzwierciedlać strukturę organizacyjną firmy, określać role odpowiedzialne za obsługę wniosków osób, których dane dotyczą (termin odpowiedzi – 30 dni), procedurę zarządzania incydentami (reakcja do 72 godzin) i być wdrożona odrębnie w każdej spółce. Dokumentacja ta stanowi kluczowy dowód rozliczalności w razie kontroli.

TYPOWY BŁĄD

Globalna polityka wdrożona „mailem", bez uchwały zarządu polskiej spółki i bez indywidualnych upoważnień; brak rejestru incydentów.

POTENCJALNE KONSEKWENCJE BŁĘDU

- Decyzja UODO 40 tys. zł za brak dokumentacji i nakaz wstrzymania przetwarzania do czasu uzupełnienia.
- Chaos operacyjny przy incydencie – brak jasnych ról spowalnia reakcję, co zwiększa ryzyko sankcji finansowych.
- W praktyce UODO najwięcej kar dotyczy właśnie braku dokumentowania naruszeń i powiadamiania osób, których dane dotyczą – np. bank ukarany na ponad 363 tys. zł za niepowiadomienie klientów o wycieku danych osobowych.

NASZA PROPOZYCJA – WARTOŚĆ DLA KLIENTA

Co dostarcza kancelaria	Wymierna korzyść
Edytowalny, skalowalny formularz upoważnień (Word/Excel)	Firma spełnia wymogi ustawy bez konieczności wymiany całej platformy IT.
Uchwała zarządu + zaktualizowana polityka ODO	Decyzje zapadają szybko i zgodnie z prawem, co minimalizuje ryzyka karne i reputacyjne.
Przegląd procedur grupowych i „lokalna nakładka" – tabela rozbieżności PL vs. standard globalny	Zespół zna procedurę w praktyce, a luki naprawia się przed realnym zgłoszeniem.
Procedura realizacji praw osób i rejestr incydentów (workflow + arkusz rejestru)	Jasny, zatwierdzony obieg wniosków i zdarzeń skraca czas reakcji, obniża ryzyko kar za opóźnienia oraz umożliwia raportowanie do zarządu w przejrzystym formacie.

7. INSPEKTOR OCHRONY DANYCH (IOD)

POLSKA SPECYFIKA

W Polsce Inspektor Ochrony Danych musi być wskazaną osobą fizyczną zgłoszoną do UODO przez polską spółkę. Jeżeli rolę tę powierzono organizacji zewnętrznej, konieczne jest wyznaczenie konkretnego pracownika tej organizacji jako odpowiedzialnego IOD. Jego dane kontaktowe – włącznie z imieniem i nazwiskiem – muszą być podane w języku polskim na stronie internetowej oraz w klauzulach informacyjnych. IOD powinien raportować bezpośrednio do zarządu i dysponować zasobami niezbędnymi do wypełniania swoich obowiązków, a także znać język polski lub mieć zapewnione wsparcie zespołu polskojęzycznego.

TYPOWY BŁĄD

Jedna osoba pełniąca funkcję globalnego DPO nie jest formalnie zgłoszona w Polsce; brak danych kontaktowych w języku polskim na stronie; IOD pełniący też inne role - konflikt interesów.

POTENCJALNE KONSEKWENCJE BŁĘDU

- Kara UODO 25 tys. zł (przykład z 2024) za brak zgłoszenia IOD.
- Możliwe kary do 2% globalnego obrotu (RODO) przy poważniejszym naruszeniu.
- Nakaz powołania nowego IOD i ponownego poinformowania wszystkich osób, których dane dotyczą.

NASZA PROPOZYCJA – WARTOŚĆ DLA KLIENTA

Co dostarcza kancelaria	Wymierna korzyść
Zgłoszenie IOD on-line w 24 h	Ryzyko kary za brak rejestracji zostaje wyeliminowane natychmiast.
Umowa outsourcingowa lub „shadow-IOD support”	Globalny DPO zyskuje lokalne wsparcie językowe i operacyjne od kancelarii, bez konieczności zatrudniania nowej osoby.
Plan roczny pracy IOD + dashboard KPI	Zarząd otrzymuje mierzalne raporty zgodności, co ułatwia nadzór i decyzje budżetowe.

8. COROCZNY PRZEGLĄD SYSTEMU OCHRONY DANYCH

POLSKA SPECYFIKA

Zgodnie z zasadą rozliczalności zawartą w art. 24 RODO, każda organizacja jest zobowiązana do przeprowadzania udokumentowanej, corocznej oceny skuteczności wdrożonych środków ochrony danych lub po każdej istotnej zmianie w środowisku IT (np. nowy system, przejęcie spółki). UODO w swoich decyzjach wymaga posiadania raportu z audytu wraz z rekomendacjami działań naprawczych zatwierdzonymi przez zarząd, co stanowi podstawę do wykazania pełnej zgodności z przepisami podczas ewentualnej kontroli.

TYPOWY BŁĄD

Polityki wdrożone w 2023 r. nie były aktualizowane, a nowe aplikacje i dostawcy nie zostały w ogóle ocenione; audyt wewnętrzny ogranicza się do checklisty „kopiuj-wklej".

POTENCJALNE KONSEKWENCJE BŁĘDU

- Nieaktualne procedury powodują, że incydenty nie są wykrywane lub zgłaszane z opóźnieniem.
- Maksymalny wymiar kary RODO w zależnosci od naruszenia wynosi 2% albo 4% globalnego obrotu.

NASZA PROPOZYCJA – WARTOŚĆ DLA KLIENTA

Co dostarcza kancelaria	Wymierna korzyść
Metodyka audytu risk-based i harmonogram 12 miesięcy	Przegląd dostosowany do realnych ryzyk biznesu, a nie „papierowa formalność".
Arkusz „audyt w 60 minut" – samoocena działów	Kierownicy poszczególnych pionów mogą szybko ocenić zgodność we własnym zakresie; centralny zespół ds. danych otrzymuje ustandaryzowane wyniki bez konieczności długich spotkań.
Warsztat „table-top" z zarządem	Kierownictwo przećwiczy scenariusz kontroli lub incydentu, co skraca czas reakcji w sytuacji krytycznej.

KONTAKT

Anna Matusiak-Wekiera

radczyni prawna | Counsel
Head of Data Protection & Compliance

E: anna.matusiak-wekiera@jdp-law.pl

Krzysztof Brant

radca prawny | Senior Associate
Data Protection & Compliance

E: krzysztof.brant@jdp-law.pl

JDP Drapała & Partners

JDP DRAPAŁA & PARTNERS Sp. k. / Numer KRS: 0001145849/ Organ rejestrujący: Sąd Rejonowy dla m. st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego / NIP: 7010056483 / REGON: 140887753