Dwa lata z RODO

Jak to wygląda w praktyce?

Katarzyna Doering

DOERING
PARTNERZY

24.11.2020 r.

RODO

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)

- Weszło w życie 04.05.2016 r.
- Zastosowanie od 25.05.2018 r.

Osoba fizyczna – kto to?

- Prawne określenie człowieka w prawie cywilnym od chwili urodzenia do chwili śmierci, w odróżnieniu od osób prawnych [Wikipedia]

Czyli kto?

- Osoba fizyczna (indywidualna, prywatna)
- Osoba fizyczna prowadząca jednoosobową działalność gospodarczą
- Osoba fizyczna będąca wspólnikiem spółki cywilnej

RODO chroni osoby fizyczne

Prawo polskie

- **Aktualnie**

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

(Dz.U. 2018 r. poz. 1000)

Obowiązuje od 25.05.2018 r.

- **Wcześniej**

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

(Dz.U. 1997 poz. 883)

Obowiązywała od 30.04.1998 r. do 24.05.2018 r.

Prawo polskie cd.

Wejście w życie wymagań RODO wymusiło zmianę **162 przepisów sektorowych**. Pakiet zmienionych aktów prawnych **wszedł w życie 04.05.2019 r.** Czyli niemalże rok po wprowadzeniu RODO. Zmiany te zostały wprowadzone **Ustawą z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO (Dz.U. 2019 poz. 730).** Oczywiście wprowadzono szereg zmian porządkujących lub dostosowujących nomenklaturę do nowych przepisów (np. zmiana GIODO na PUODO), ale w dużej części ustaw wprowadzono znaczące zmiany i uregulowania. Dostosowano do RODO przepisy z zakresu prawa pracy, prawa oświatowego, prawa konsumenta, prawa pacjenta, prawa bankowego i ubezpieczeniowego oraz z zakresu usług płatniczych, telekomunikacyjnych czy postępowania administracyjnego.

Kodeksy postępowania

- Zgodnie z art. 40 RODO zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających mogą opracowywać kodeksy postępowania mających pomóc we właściwym stosowaniu rozporządzenia.
- Nadzór nad prawidłowym stosowaniem kodeksu postępowania pełni podmiot monitorujący.
- Podmiot monitorujący przestrzeganie kodeksu postępowania uzyskuje akredytację od Prezesa UODO.
- Podmiot monitorujący odpowiada za nadzorowanie przestrzegania zawartych w kodeksie postępowania przepisów, w tym ocenia zdolność aplikanta do stosowania kodeksu oraz rozpatruje skargi na naruszanie kodeksu.

Kodeksy postępowania cd.

0

Procedura zatwierdzania kodeksu postępowania:

1) Przygotowanie projektu kodeksu postępowania.
2) Przedłożenie projektu do konsultacji.
3) Przedstawienie projektu kodeksu postępowania wraz z informacją o przeprowadzonych konsultacjach i wynikach konsultacji Prezesowi Urzędu Ochrony Danych Osobowych.
4) Prezes UODO przedstawia opinię o zgodności projektu kodeksu z RODO i zatwierdza go, jeżeli uzna, że stanowi on odpowiednie zabezpieczenie.
5) Zatwierdzony kodeks wprowadzony jest do rejestru zatwierdzonych kodeksów postępowania. Rejestr prowadzony jest przez Prezesa UODO.

Kodeksy postępowania cd.

Złożone do Prezesa UODO projekty kodeksów postępowania:

1) *Kodeks postępowania RODO dla małych placówek medycznych* – Porozumienie Zielonogórskie.
2) *Kodeks dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe - Zw*iązek Banków Polskich.
3) *RODO w sektorze medycznym* – Polska Federacja Szpitali.
4) *Kodeks dobrych praktyk w zakresie przetwarzania danych osobowych przez spółdzielnie mieszkaniowe* – Związek Rewizyjny Spółdzielni Mieszkaniowych RP.

Kodeksy postępowania cd.

Złożone do PUODO projekty kodeksów postępowania:

5) *Kodeks postępowania KIDP w zakresie danych osobowych* - Krajowa Izba Doradców Podatkowych.
6) *Kodeks postępowania w zakresie ochrony i przetwarzania danych osobowych w badaniach rynku i opinii* – Związek Pracodawców Organizacja Firm Badania Opinii i Rynku.
7) *Kodeks RODO dla sektora handlowego* - Polska Rada Centrów Handlowych.
8) *Kodeks postępowania dla bibliotek wspierający we właściwym stosowaniu RODO* - Stowarzyszenie Bibliotekarzy Polskich.

Kodeksy postępowania cd.

Inicjatywy opracowania kodeksów postępowania:

1) *Kodeks postępowania dla fotografów.*
2) *Kodeks postępowania i dobrych praktyk w zakresie ochrony danych osobowych w działaniach marketingu bezpośredniego.*
3) *Kodeks postępowania w zakresie ochrony danych osobowych dla uczelni medycznych.*
4) *Kodeks postępowania i dobrych praktyk w zakresie przetwarzania danych osobowych w branży reklamy internetowej.*

Kodeksy postępowania cd.

Inicjatywy opracowania kodeksów postępowania:

5) *Kodeks postępowania w zakresie przetwarzania danych osobowych w organizacjach społecznych.*
6) *Kodeks dotyczący zasad przetwarzania danych osobowych gości hotelowych.*
7) *Kodeks ochrony danych osobowych w rekrutacji.*
8) *Kodeks postępowania dla jednostek oświatowych, mający na celu doprecyzowanie stosowania rozporządzenia 2016/679.*

Plan kontroli

- Urząd Ochrony Danych Osobowych na początku roku przedstawia plan kontroli sektorowych na dany rok.
- Plan kontroli dostępny jest na stronie UODO.
- Poza kontrolami sektorowymi (planowanymi) Urząd Ochrony Danych Osobowych przeprowadza również kontrole doraźne.
- Zakres kontroli: wymagania zawarte w RODO.

Plan kontroli 2020 r.

1) **Organy przetwarzające dane osobowe w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym**, w tym audyt bezpieczeństwa SISII/VIS: konsulaty i organy administracji skarbowej w zakresie przetwarzania danych osobowych SISII i VIS.
2) **Banki** – przetwarzanie danych osobowych w związku ze sporządzaniem kopii/skanów dokumentów tożsamości klientów i potencjalnych klientów.
3) **Podmioty korzystające z systemu zdalnego odczytu wodomierzy (tzw. Inteligentne czytniki)** – przetwarzanie danych osobowych w związku z korzystaniem z tych wodomierzy.

Zasady kontroli

1) Kontrole przeprowadzane są przez upoważnionych pracowników UODO oraz upoważnionych członków lub pracowników organu nadzorczego państwa członkowskiego UE.
2) Kontrolę przeprowadza się po okazaniu imiennego upoważnienia wraz z legitymacją służbową lub dokumentem potwierdzającym tożsamość w przypadku pracowników organu nadzorczego państwa członkowskiego UE.
3) Czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej.

Zasady kontroli cd.

4) Kontrolujący ma prawo:

- wstępu w godzinach od 6.00 do 22.00 na grunt oraz do budynków, lokali lub innych pomieszczeń;
- wglądu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;
- przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
- żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;
- zlecać sporządzanie ekspertyz i opinii.

Zasady kontroli cd.

5) Kontrolowany w terminie 7 dni od dnia przedstawienia protokołu kontroli do podpisu podpisuje go albo składa pisemne zastrzeżenia co do jego treści.
6) Kontrolę prowadzi się nie dłużej niż 30 dni od dnia okazania kontrolowanemu lub innej osobie wskazanej w przepisach imiennego upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej lub innego dokumentu potwierdzającego tożsamość. Do terminu nie wlicza się terminów przewidzianych na zgłoszenie zastrzeżeń do protokołu kontroli lub podpisanie i doręczenie protokołu kontroli przez kontrolowanego.
7) Terminem zakończenia kontroli jest dzień podpisania protokołu kontroli przez kontrolowanego lub dzień dokonania wzmianki o odmowie podpisania.

Kontrole

- **Kontrole sektorowe** kontrole przeprowadzone zgodnie z planem kontroli Prezesa UODO.
- **Kontrole doraźne** zainicjowane są skargami bądź sygnałami od obywateli, a także przesłanymi przez administratorów naruszeniami ochrony danych osobowych czy doniesieniami medialnymi.

Okres	Ilość kontroli sektorowych i doraźnych
2018, w tym 25.05.2018 – 31.12.2018	72, w tym 32
2019	98

Skargi

- Do Urzędu Ochrony Danych Osobowych wpływają skargi, które rozpatrywane są w trybie Kodeksu postępowania administracyjnego.
- Postępowania te kończą się wydaniem decyzji administracyjnej, mocą której Prezes UODO m.in. umarza postępowanie, odmawia uwzględnienia wniosku skarżącego, nakazuje przywrócenie stanu zgodnego z prawem, nakłada karę, upomnienie albo ostrzeżenie na administratora czy podmiot przetwarzający.

Okres	Ilość złożonych skarg	Ilość zakończonych postępowań administracyjnych
2018, w tym 25.05.2018 – 31.12.2018	5565, w tym 4550	527
2019	9304	1369

Naruszenia odo

- **Naruszenie ochrony danych osobowych** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzany.
- **Naruszenie ochrony danych osobowych** zgłaszane do Prezesa UODO w ciągu 72 h przez administratora.

Okres	Ilość zgłoszonych naruszeń ochrony danych osobowych
25.05.2018 – 31.12.2018	2446
2019	6039

Nieprawidłowości

1) Niewłaściwe dopełnianie obowiązku informacyjnego wobec osób, których dane dotyczą.
2) Nieujmowanie w rejestrze czynności przetwarzania wszystkich wymaganych czynności oraz błędne określanie okresu retencji danych.
3) Nie zawieranie umów powierzenia przetwarzania danych.
4) Problemy z właściwym przeprowadzaniem analizy ryzyka i oceny skutków dla ochrony danych.
5) Nienadawanie stosownych uprawnień do przetwarzania danych osobowych.
6) Brak polityki ochrony danych osobowych.

Nieprawidłowości cd.

7) Niewdrożenie odpowiednich środków technicznych i organizacyjnych mających na celu zabezpieczenie danych zapisywanych na nośnikach elektronicznych.
8) Zgłoszenie organowi nadzorczemu naruszeń ochrony danych osobowych jedynie w przypadku, w którym w ocenie podmiotu kontrolowanego, nie wystąpiło wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą.
9) Brak odpowiedzi podmiotu kontrolowanego na pisma Prezesa UODO.
10) Uniemożliwienie osobom kontrolującym wejścia do siedziby podmiotu kontrolowanego i nieudostępnienie dokumentów.

Administracyjne kary pieniężne

- **Bisnode Polska sp. z o.o.** – za niedopełnienie obowiązku informacyjnego wobec 6,6 mln osób – 943 tys. PLN
- **Dolnośląski Związek Piłki Nożnej** – ujawnienie na stronie internetowej danych osobowych 585 osób posiadających licencje sędziowskie – ponad 55 tys. PLN
- **Morele.Net sp. z o.o.** – wyciek danych ponad 2 mln osób – ponad 2,83 mln PLN
- **ClickQuickNow sp. z o.o.** – utrudnienie realizacji prawa do wycofania zgody na przetwarzanie danych osobowych – ponad 201 tys. PLN
- **Burmistrz miasta Aleksandrów Kujawski** – brak umowy powierzenia przetwarzania danych – 40 tys. PLN
- **Wspólnota mieszkaniowa** – przetwarzanie danych w ramach monitoringu wizyjnego – 2 tys. PLN
- **Spółka zarządzająca nieruchomościami** – przetwarzanie danych w ramach monitoringu wizyjnego – 8 tys. PLN
- **Spółka zajmująca się ochroną osób i mienia** – przetwarzanie danych w ramach monitoringu wizyjnego – 30 tys. PLN

Administracyjne kary pieniężne

- **SP2 w Gdańsku** – przetwarzania linii papilarnych osób korzystających ze stołówki – 20 tys. PLN
- **Vis Consulting sp. z o.o.** – uniemożliwienie przeprowadzenia czynności kontrolnych przez Prezesa UODO – 20 tys. PLN
- **East Power sp. z o.o.** – nieudzielenie informacji – 15 tys. PLN
- **Pani A.T. prowadząca działalność gospodarczą** – nieudzielnie informacji – 5 tys. PLN
- **Główny Geodeta Kraju** – udostępnienie danych bez podstawy prawnej na portalu GEOPORTAL2 – 100 tys. PLN
- **SGGW** – naruszenie ochrony danych, w tym braki w dokumentacji oraz przeprowadzonych procesach – 50 tys. PLN

Praca zdalna

- Na podstawie przepisów wprowadzanych w związku z pandemią COVID-19 (**Ustawa z 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych innymi sytuacjami kryzysowymi**).
- Praca zdalna nie jest równoznaczna z telepracą, o której mowa w Kodeksie pracy.
- Nowelizacja Kodeksu pracy, która pozwoli na stałe wprowadzić instytucję pracy zdalnej do przepisów krajowych.
- Wewnętrzne uregulowania – procedura/instrukcja pracy zdalnej.

Praca zdalna

1) **Polecenie pracodawcy wykonania pracy zdalnej przez pracownika:**
   - Ze względów porządkowych i dowodowych wskazane jest, aby polecenie miało formę pisemną.
   - Określony okres wykonywania pracy zdalnej oraz wskazane miejsce wykonywania.
   - Do pracy zdalnej może być skierowany pracownik, który ma umiejętności i możliwości techniczne oraz lokalowe. Jeżeli pracownik nie ma możliwości pracować zdalnie ze względu na warunki lokalowe, nie można powierzyć mu takiej formy pracy.
   - Pracownik nie musi wykonywać pracy zdalnej w swoim miejscu zamieszkania, jednak wskazane jest, aby pracodawca znał miejsce wykonywania pracy zdalnej.
   - Pracownik nie może odmówić polecenia wykonania pracy zdalnej – mogą grozić mu kary porządkowe zgodnie z Kodeksem pracy.
   - Poinformowanie pracownika o zasadach wykonywania pracy zdalnej.

Praca zdalna

2) Narzędzia do wykonywania pracy zdalnej:

- Pracodawca zobowiązany jest dostarczyć pracownikowi narzędzia i materiały do pracy zdalnej oraz obsługę logistyczną.
- Pracownik może używać do pracy zdalnej narzędzia lub materiały niezapewnione przez pracodawcę pod warunkiem, że będzie to umożliwiało poszanowanie i ochronę informacji poufnych i innych tajemnic prawnie chronionych, w tym tajemnic przedsiębiorstwa lub danych osobowych, a także informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.
- Pracodawca może porozumieć się z pracownikiem, aby pracownik pracował na prywatnym sprzęcie informatycznym, pod warunkiem dostępu do wewnętrznej sieci pracodawcy.

Praca zdalna

3) Ewidencja wykonywania czynności:

- Pracownik zobowiązany jest do prowadzenia ewidencji czynności, uwzględniającą w szczególności formę pracy zdalnej, opis tych czynności, a także datę oraz czas ich wykonania.
- Pracodawca w poleceniu pracy zdalnej określa formę ewidencji i częstotliwość jej przekazania.

Praca zdalna

4) Ochrona danych osobowych:

- Zapewnienie właściwego poziomu bezpieczeństwa.
- Niewykonywanie pracy w miejscach publicznych.
- Wykorzystanie najlepiej tylko narzędzi udostępnionych przez pracodawcę (służbowy telefon i e-mail oraz sieć pracodawcy i łączenie się z siecią za pomocą bezpiecznego łącza VPN).
- Praca na dokumentach elektronicznych dostępnych poprzez sieć pracodawcy.
- Praca na kopiach dokumentów papierowych. Zgoda pracodawcy na wykonanie kopii. Spis kopii dokumentów. Zwrot kopii dokumentów pracodawcy po ich wykorzystaniu.
- Zabezpieczenie dokumentów i sprzętu informatycznego przed dostępem osób postronnych.
- Zgłaszanie wszelkich nieprawidłowości pracodawcy lub osobie wyznaczonej.

Dziękuję za uwagę

Katarzyna Doering

Doering & Partnerzy

tel. 600 210 513

e-mail: katarzyna@doering-partnerzy.pl

www.doering-partnerzy.pl

DOERING

PARTNERZY