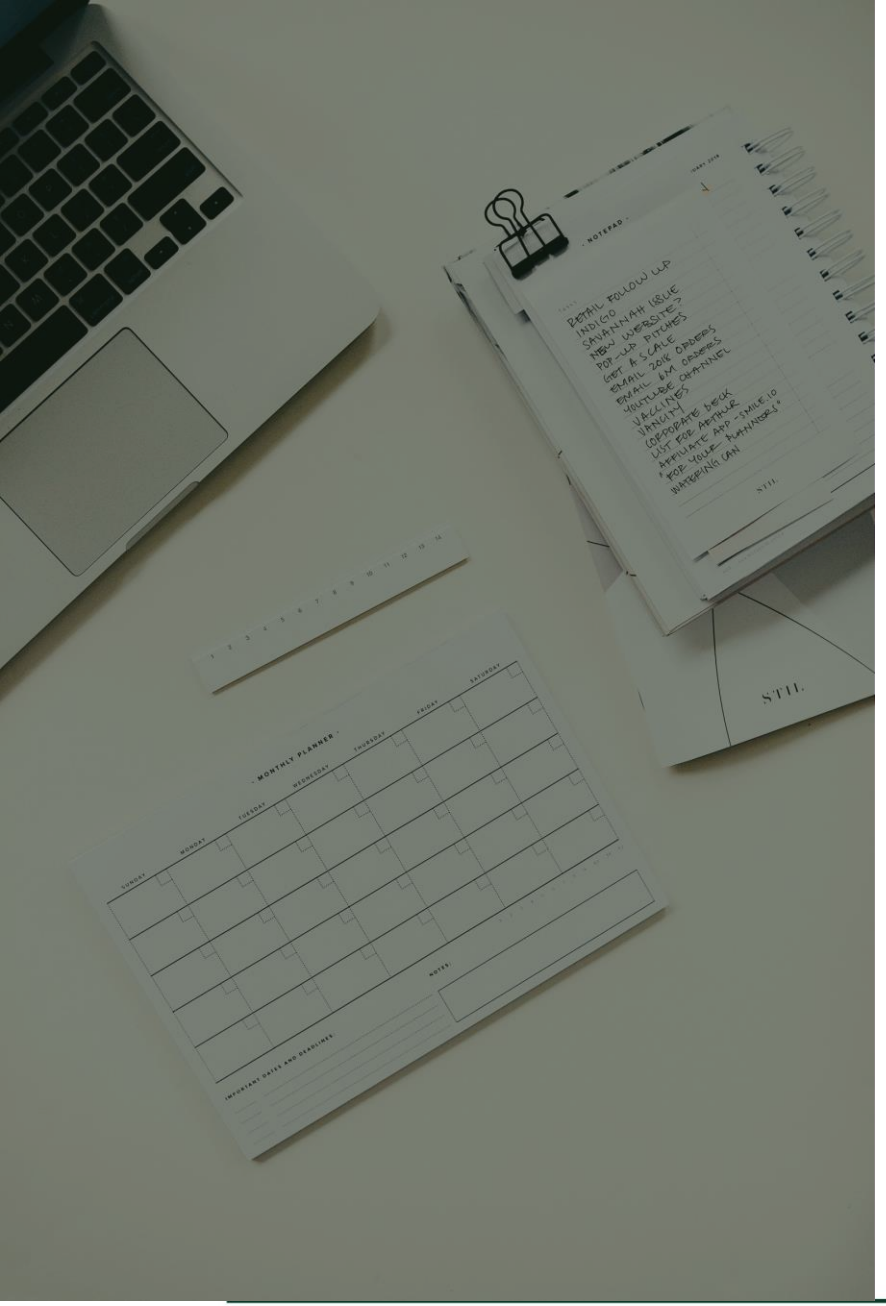
DAWID & PARTNERZY
ADWOKACI I RADCOWIE PRAWNI

Dostosowanie prawa polskiego do RODO – jak przebiegał proces legislacyjny?



Agenda

1. RODO – informacje ogólne
2. Ustawa o ochronie danych osobowych
3. Proces ustawodawczy – UODO
4. D&P – dane kontaktowe

RODO – ogólna charakterystyka

1. RODO – **Rozporządzenie Ogólne o Ochronie Danych Osobowych**

2. Rozporządzenie unijne (**Parlament Europejski i Rada UE**)

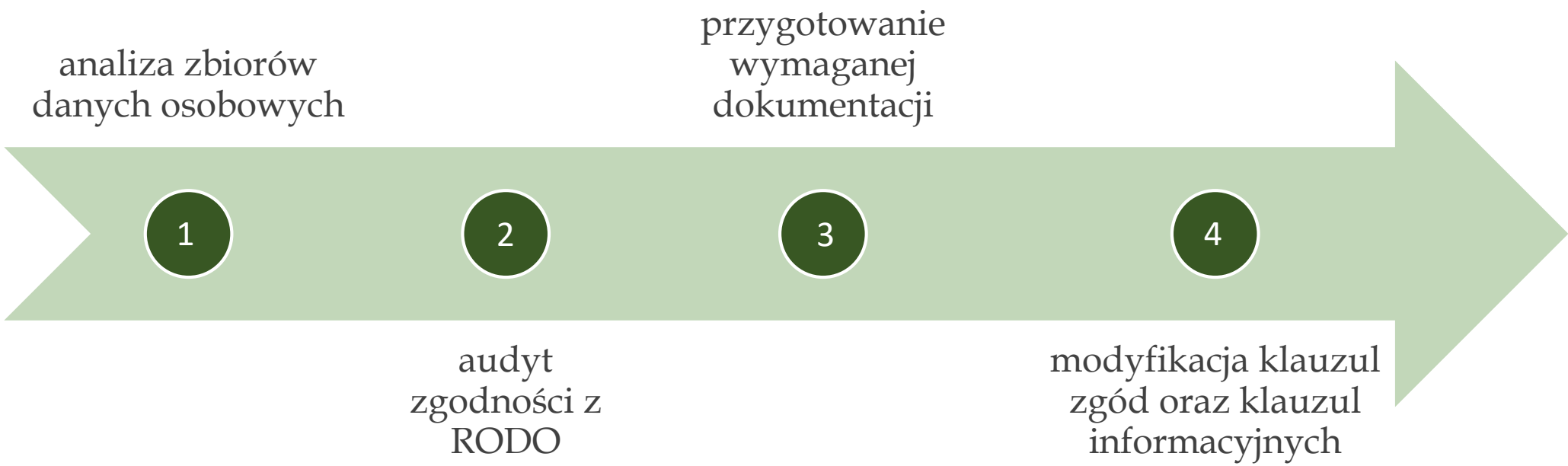
3. wiąże w całości od **25 maja 2018 r.**

RODO – ogólna charakterystyka

4 największa reforma ochrony danych osobowych od 21 lat

5 konieczność wdrożenia przez polskie przedsiębiorstwa szeregu zmian o charakterze prawnym i informatycznym

Wdrożenie RODO – plan działania



Wymagana dokumentacja

1. brak wskazania w RODO niezbędnej dokumentacji
2. brak wskazania treści dokumentacji
3. stworzenie dokumentacji leży w gestii podmiotu
4. obowiązek dokumentowania czynności przetwarzania danych osobowych

Wymagana dokumentacja

5 zaktualizowany dokument „Polityka bezpieczeństwa”

6 rejestr czynności przetwarzania danych osobowych

7 inne, dostosowane indywidualnie

Przetwarzanie danych osobowych

Wszelkie operacje na danych osobowych dokonywane w sposób zautomatyzowany lub niezautomatyzowany, tj.:

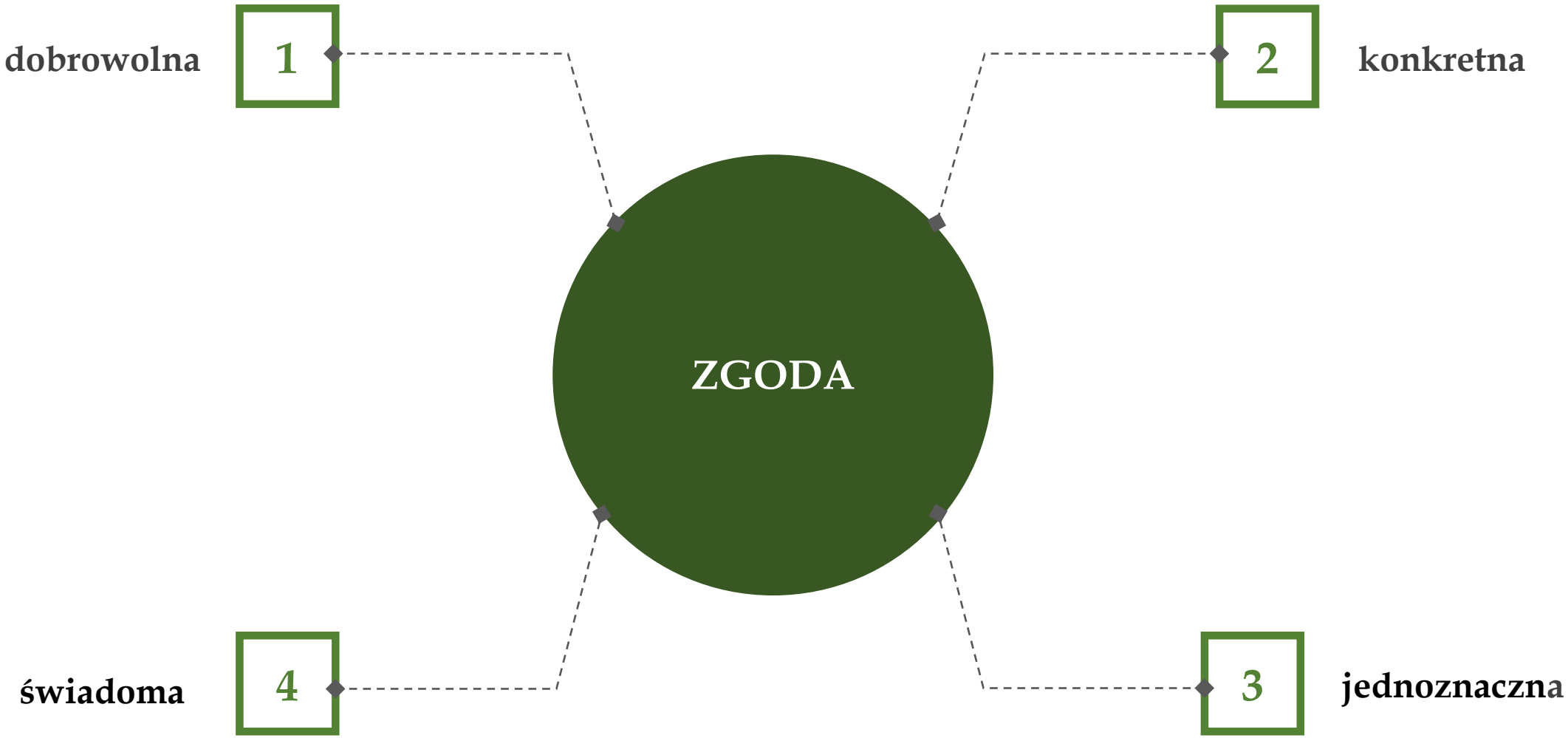
1. zbieranie
2. utrwalanie
3. organizowanie
4. porządkowanie
5. przechowywanie
6. adaptowanie lub modyfikowanie
7. pobieranie
8. wykorzystywanie i przeglądanie
9. ujawnianie przez przesyłanie lub innego rodzaju udostępnianie
10. łączenie, dopasowywanie, ograniczenie, usuwanie i niszczenie

Przetwarzanie danych osobowych

1. na podstawie normy prawnej (prawa UE lub państwa członkowskiego np. Kodeks pracy)

2. zgoda (oświadczenie lub wyraźne działanie) osoby, której dane dotyczą

Przetwarzanie danych osobowych



Przetwarzanie danych osobowych

Zgodne z prawem również, gdy niezbędne do:

- wykonania umowy
- podjęcia działań na żądanie osoby, której dane dotyczą
- wypełnienia obowiązku prawnie ciążącego na administratorze
- ochrony żywotnych interesów osoby, której dane dotyczą
- celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub osobę trzecią

Administrator

osoba fizyczna

organ publiczny

osoba prawna

lub inny podmiot, który
samodzielnie lub wspólnie
z innym (współadministratorzy)
ustala cele i sposoby przetwarzania
danych osobowych

Różnice pomiędzy administratorem a procesorem

Podmiot przetwarzający / procesor

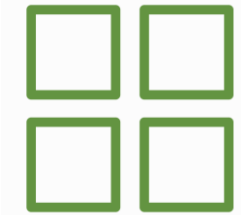
- przetwarza w imieniu administratora
- obowiązek administratora wyboru odpowiedniego procesora (gwarancja ochrony danych osobowych)
- zgoda administratora – uprzednia, pisemna, jednoznaczna

Administrator a procesor

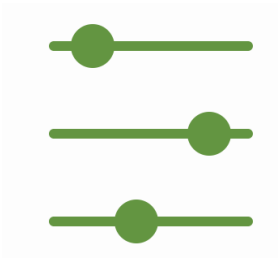
- kwestia decydowania o środkach i celach przetwarzania danych osobowych
- obowiązek zawarcia umowy powierzenia przetwarzania danych osobowych

Umowa powierzenia przetwarzania

przedmiot i czas trwania



kategorie osób, które dane dotyczą



rodzaj danych osobowych

charakter i cel przetwarzania

obowiązki i prawa administratora

Obowiązki informacyjne Administratora

Obowiązki administratora

1. dane administratora i dane kontaktowe (przedstawiciela, IOD)
2. cel i podstawa prawna przetwarzania
3. odbiorcy danych
4. zamiar przekazania do państwa trzeciego lub organizacji międzynarodowej
5. okres, przez jaki będą przechowywane
6. pouczenie o prawie modyfikacji, uaktualnienia, ograniczenia przetwarzania, usunięcia bycia zapomnianym, wniesienia skargi do PUODO
7. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu

Sankcje w RODO - maksymalne wysokości kar pieniężnych

OSOBY FIZYCZNE

- do **10 000 000 euro**

lub

- do **20 000 000 euro**

PRZEDSIĘBIORCY

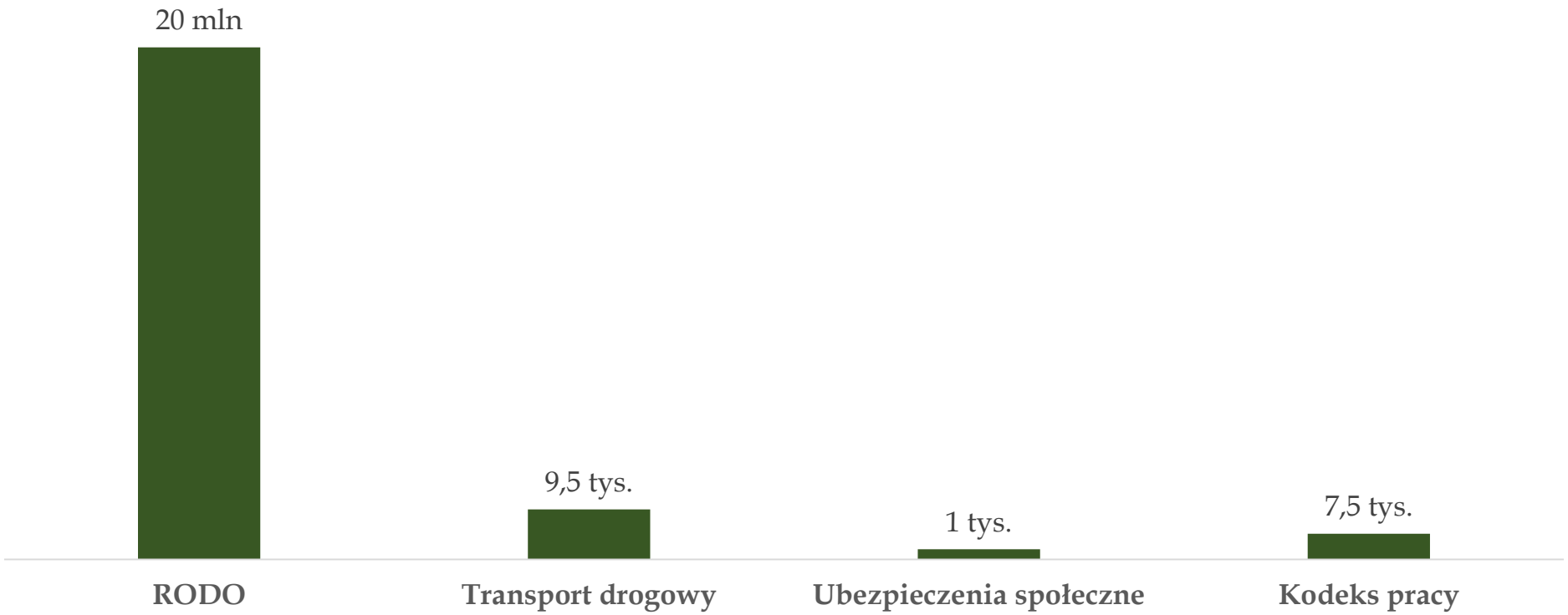
- do **2% całkowitego rocznego globalnego obrotu** z poprzedniego roku obrotowego lub do **10 000 000 euro**

lub

- do **4% całkowitego rocznego globalnego obrotu** z poprzedniego roku obrotowego lub do **20 000 000 euro**

Kary z RODO na tle innych kar

Maksymalne wysokości kar pieniężnych za naruszenia przepisów ustawy*



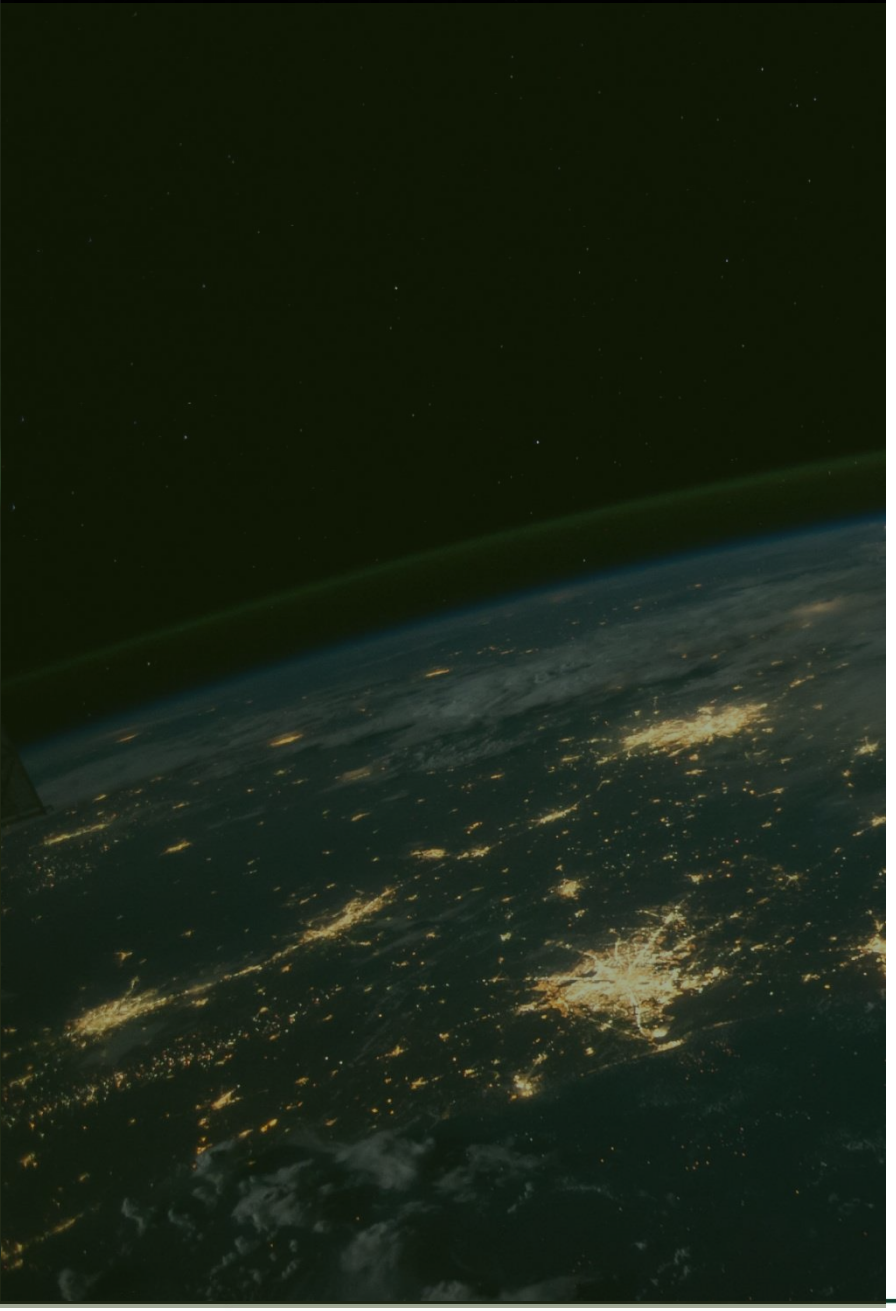
*Powyższe kwoty podane są w EUR według kursu 1 EUR = 4,27 PLN

Inne sankcje w RODO

1. odszkodowanie za poniesioną szkodę dla pokrzywdzonego
2. ostrzeżenia, upomnienia
3. zakaz lub ograniczenie przetwarzania danych osobowych
3. nakazy

Dlaczego wprowadzono tak wysokie kary?

- coraz częstsze wycieki danych na skalę światową
- wzmożona ochrona osób fizycznych
- drakońskie sumy wynikiem zaniedbań ze strony firm
- zwrócenie uwagi na problem ochrony danych osobowych



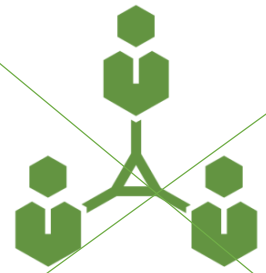
Największe wycieki danych w Polsce

- przejęcie danych osobowych z 4 banków w Polsce (dane ponad 3000 osób)
- wyciek danych z systemu InPost (dane ponad 5000 osób)
- wyciek bazy danych z firmy Uber
- wyciek bazy danych z firmy Netia
- wyciek bazy danych z firmy wonga.com

Kontrole przedsiębiorców

PUODO

- od teraz prowadzone przez nowy organ – **Prezesa Urzędu Ochrony Danych Osobowych**
- planowany ok. **500** osobowy zespół inspektorów do egzekucji **RODO**



GIODO

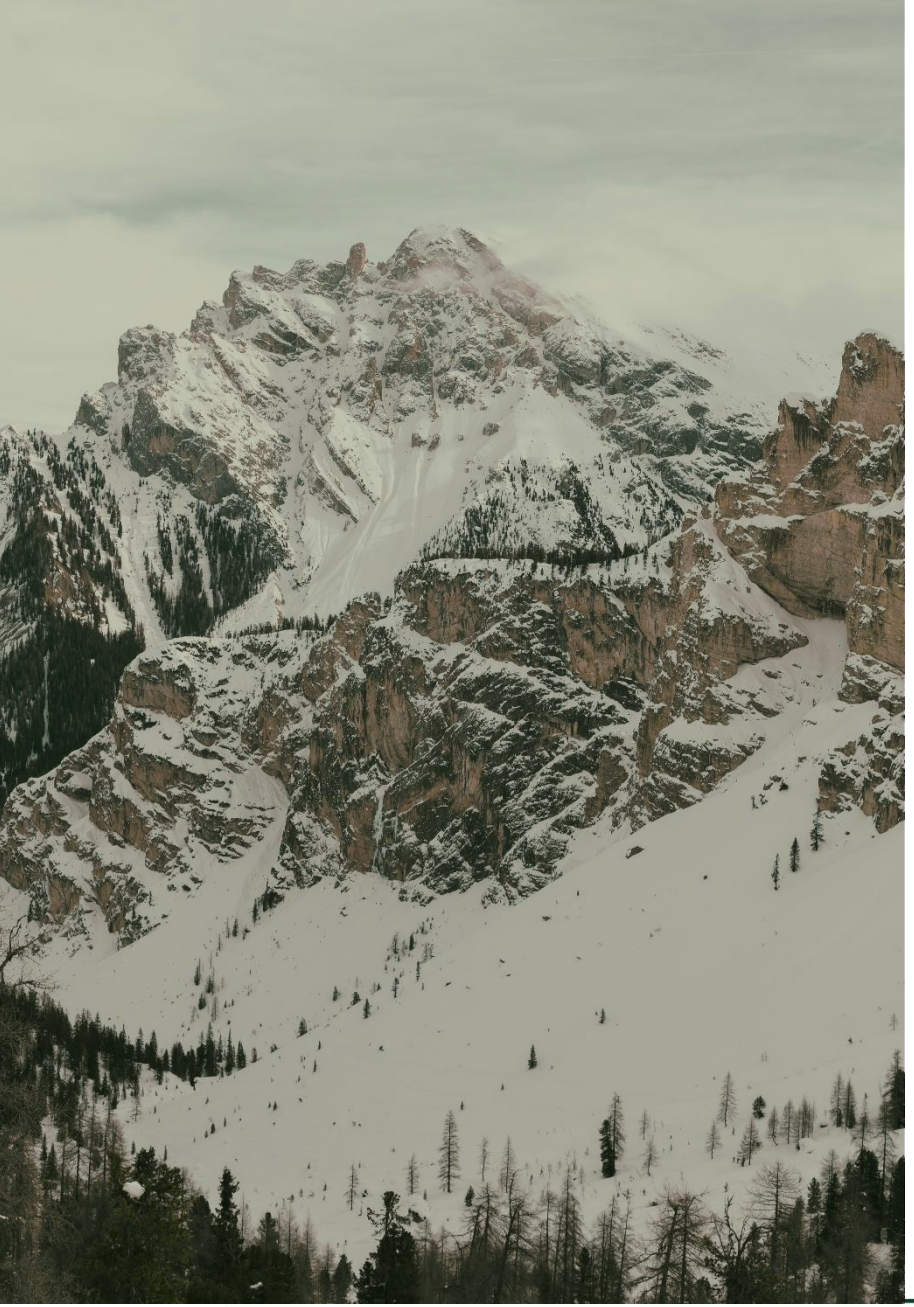
- wcześniej prowadzone przez **Generalnego Inspektora Ochrony Danych Osobowych**
- wcześniej zespół składał się z **ok. 30** kontrolerów

Kontrole przedsiębiorców

policja

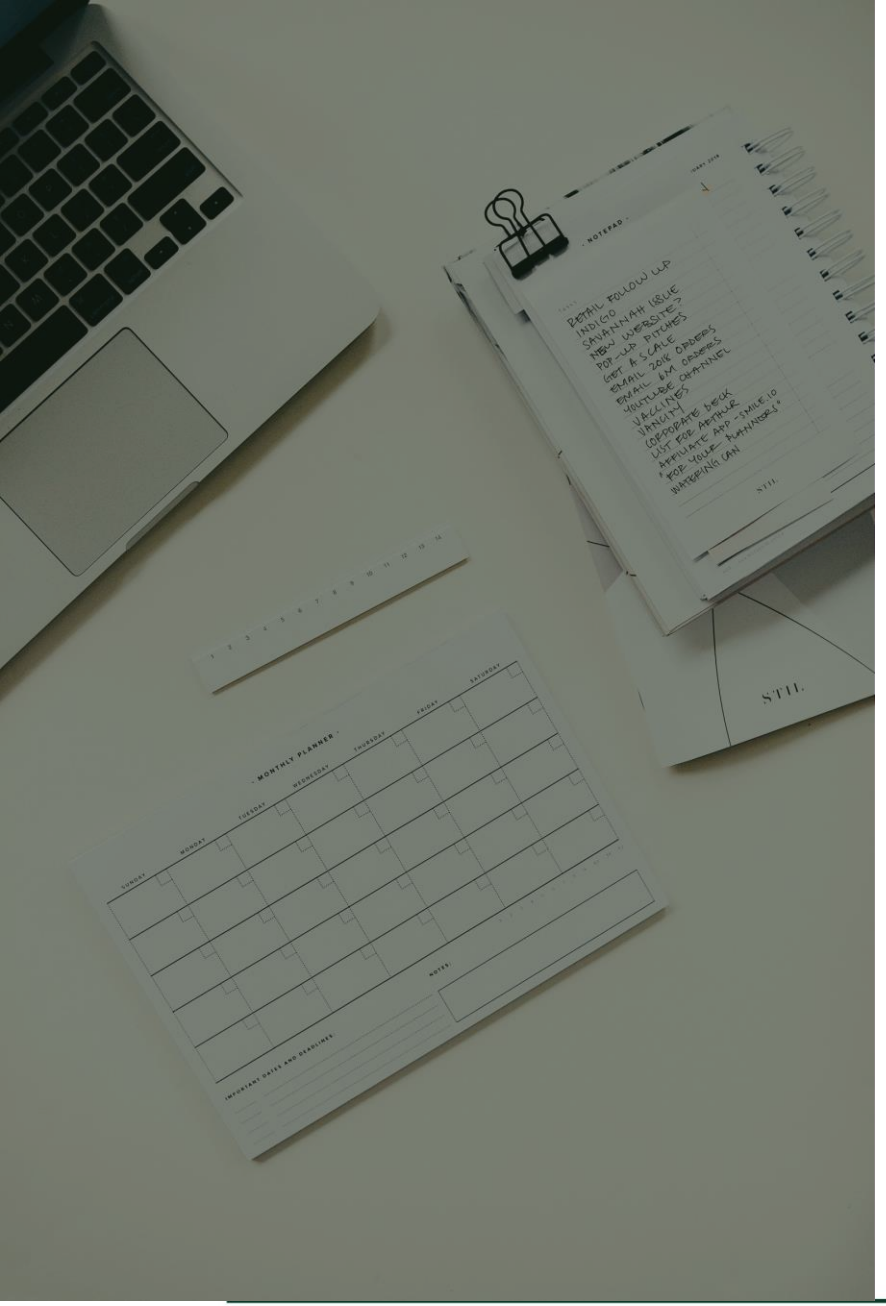
miesiąc

kontroler z dużymi uprawnieniami



Zagrożenia i wyzwania wdrożenia RODO

1. realna perspektywa **wielomilionowych kar**
2. konieczność zaprojektowania całego **systemu ODO**
3. konieczność wytworzenia w przedsiębiorstwach **mechanizmów i dokumentów** zgodnych z RODO
4. konieczność skrupulatnego prowadzenia **rejestru danych osobowych** z generowaniem pliku PDF/Excel/Word
3. konieczność **zgłaszania incydentów** np. w wyniku ataku hakerskiego w ciągu 72 h.



Agenda

1. RODO – informacje ogólne
2. Ustawa o ochronie danych osobowych
3. Proces ustawodawczy – UODO
4. D&P – dane kontaktowe

Dotychczasowa ustawa o ochronie danych osobowych a RODO

Definicja przetwarzania danych osobowych:

Zgodnie z RODO:

„przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Zgodnie z polską Ustawą:

rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Dotychczasowa ustawa o ochronie danych osobowych a RODO

sankcje

zgłaszanie wycieków danych osobowych

ABI / IOD

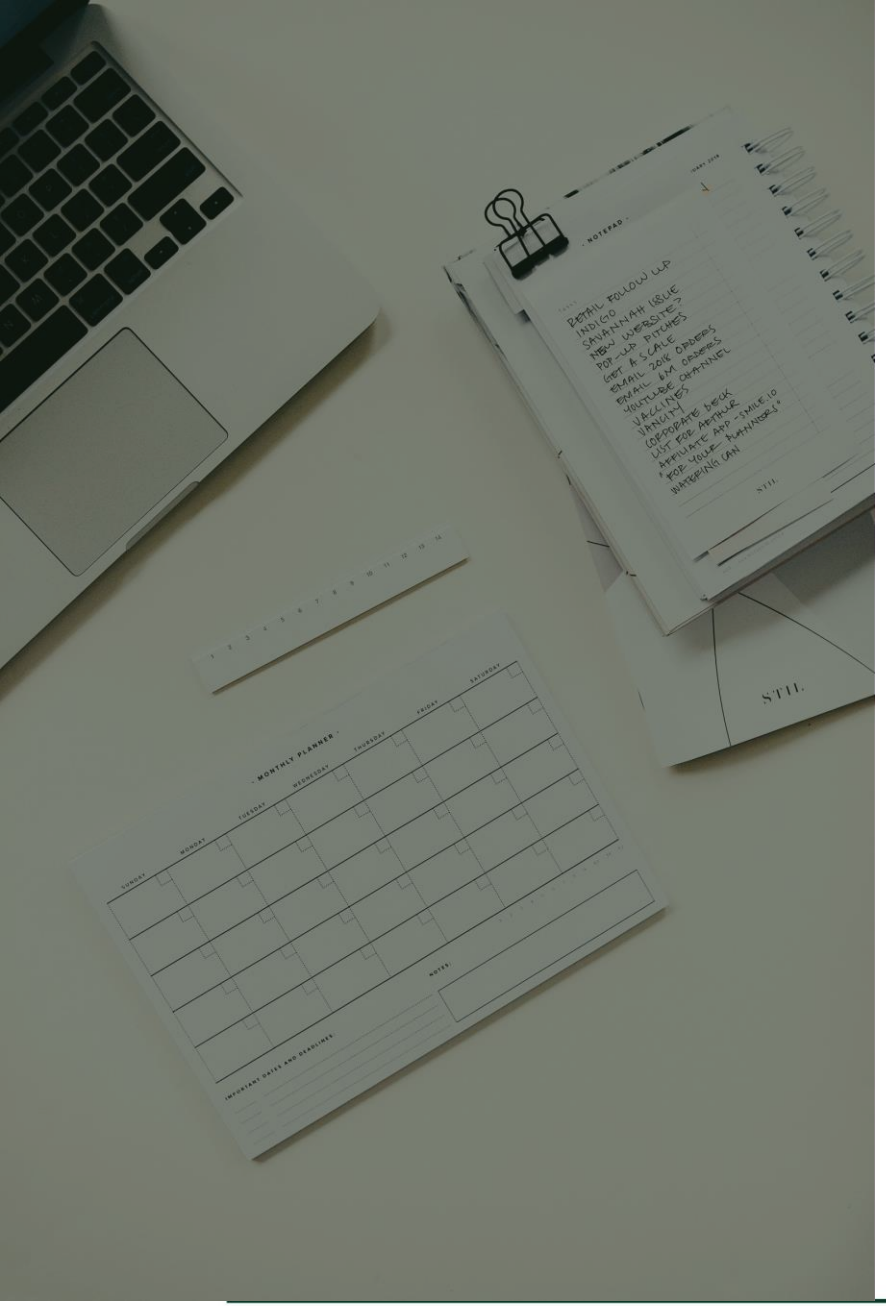
zbiór danych osobowych

Nowa ustawa o ochronie danych osobowych

RODO zacznie obowiązywać niezależnie od wejścia w życie polskiej ustawy

Najważniejsze zmiany:

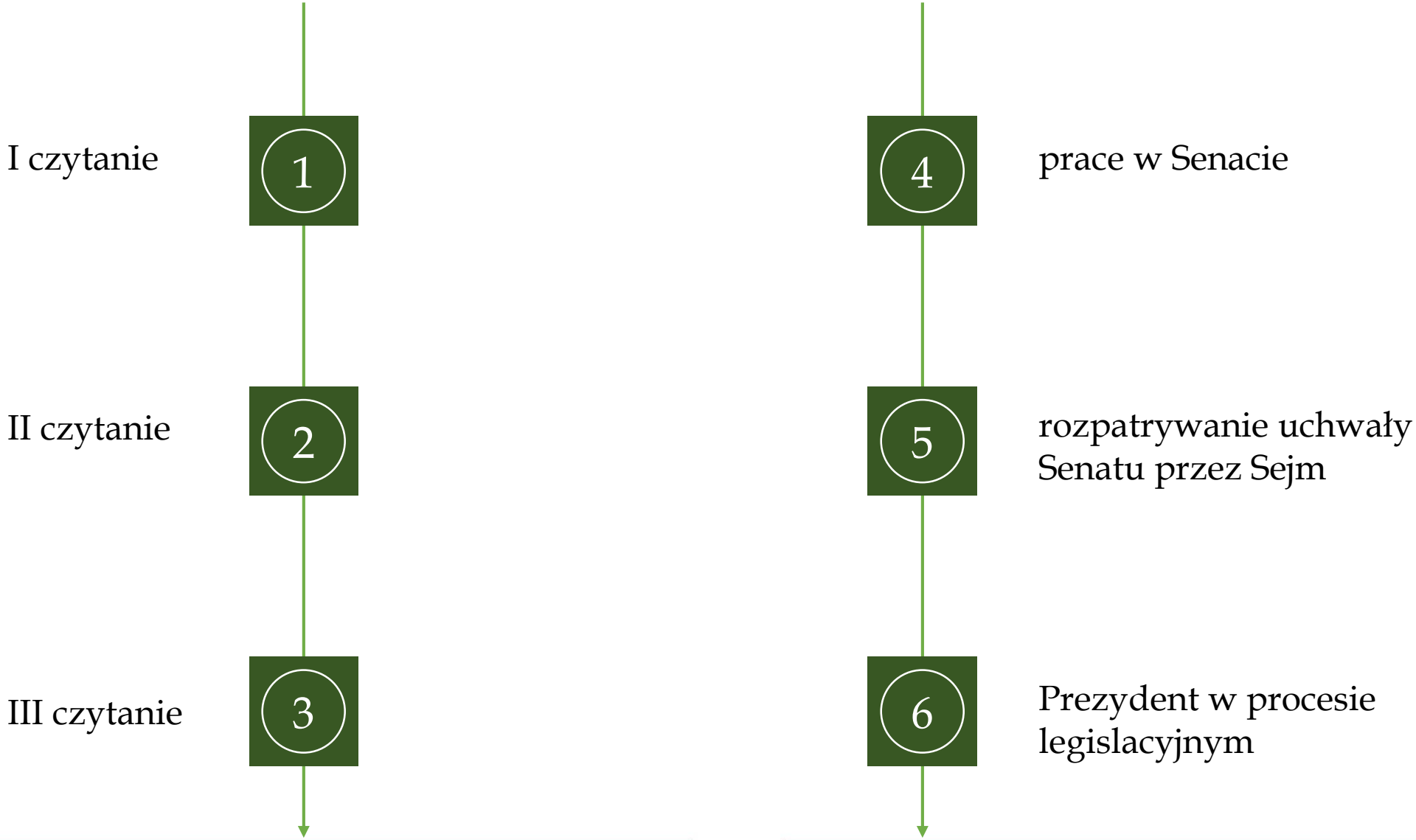
1. PUODO zamiast GIODO
2. certyfikaty
3. uprawnienia kontrolera
4. zmiany w Kodeksie Pracy



Agenda

1. RODO – informacje ogólne
2. Ustawa o ochronie danych osobowych
3. Proces ustawodawczy – UODO
4. D&P – dane kontaktowe

Proces ustawodawczy



Ustawa o działalności lobbingowej w procesie stanowienia prawa

Definicja działalności lobbingowej

„każde działanie prowadzone metodami prawnie dozwolonymi zmierzające do wywarcia wpływu na organy władzy publicznej w procesie stanowienia prawa”

- zasady jawności działalności lobbingowej w procesie stanowienia prawa
- wykaz prac legislacyjnych
- udostępnienie w Biuletynie Informacji Publicznej
- zgłoszenie zainteresowania pracami
- wysłuchanie publiczne

Ustawa o ochronie danych osobowych – wersje projektów

12.09.2017 r. 08.02.2018 r. 03.03.2018 r. 16.03.2018 r. 27.03.2018 r.

Zmiany w projektach ustawy

- rozumienie organów i podmiotów publicznych
- certyfikacja
- kandydat na PUODO
- rozszerzenie przepisów karnych
- wyłączenie podmiotów zatrudniających poniżej 250 os.

Etapy przy opracowywaniu projektów

uzgodnienia

konsultacje publiczne

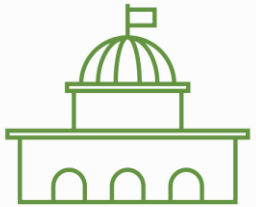
opiniowanie

Komitet do Spraw Europejskich

Stały Komitet Rady Ministrów

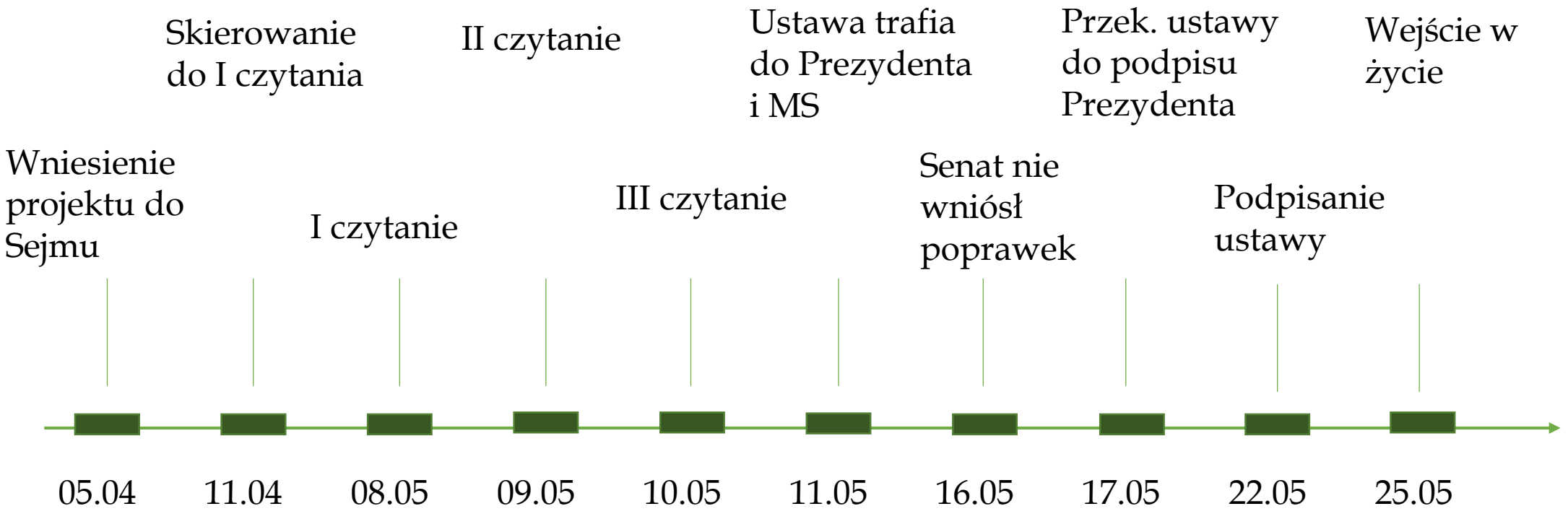
Komisja Prawnicza

Rada Ministrów



skierowanie projektu ustawy do sejmu

Prace w Sejmie



Obowiązywanie ustawy o ochronie danych osobowych

Traci moc ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138 i 723)

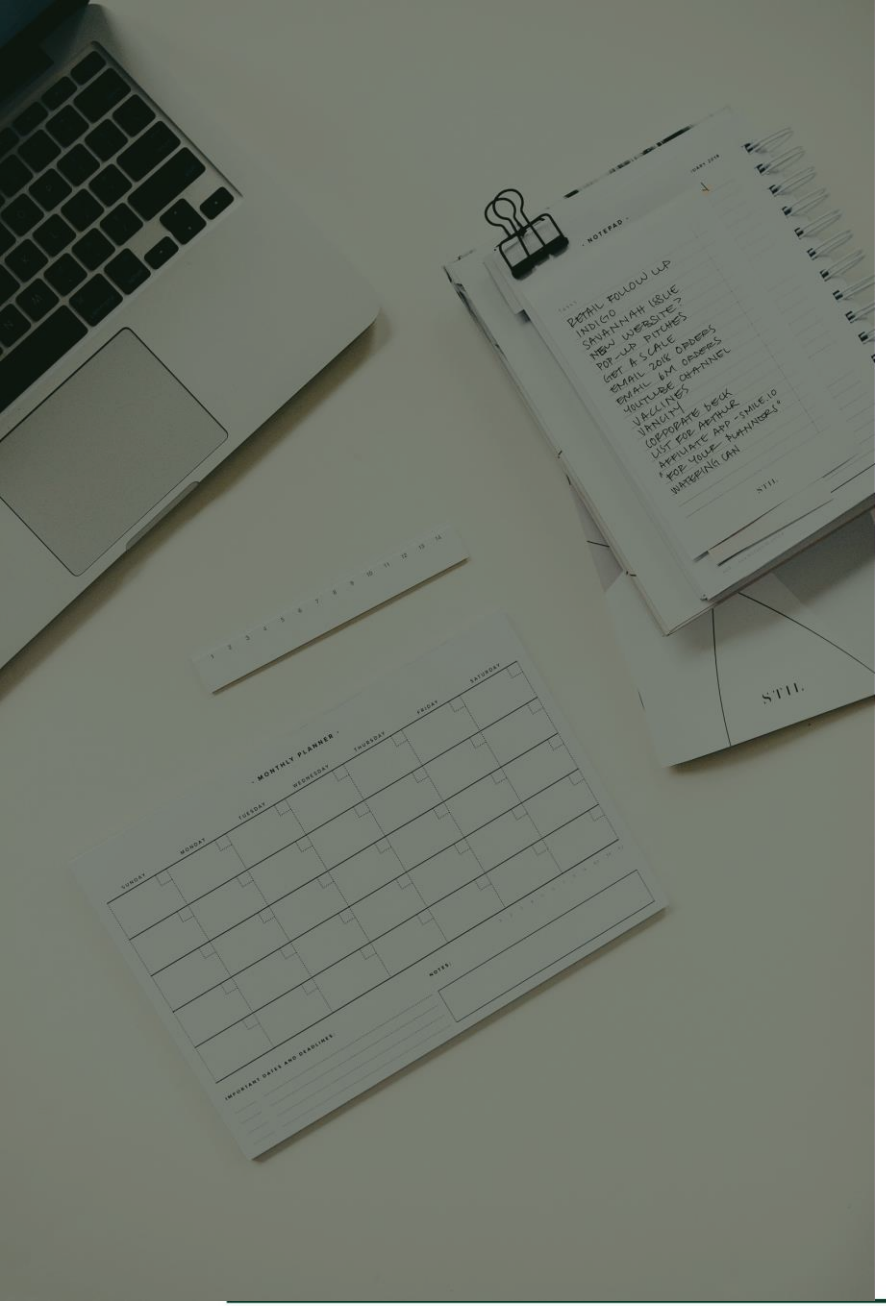
z wyjątkiem art. 1, art. 2, art. 3 ust. 1, art. 4–7, art. 14–22, art. 23–28, art. 31 oraz rozdziałów 4, 5 i 7

które zachowują moc w odniesieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie.

W terminie do dnia wejścia w życie przepisów wdrażających dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW.

Przepisy wprowadzające ustawę o ochronie danych osobowych

- zmiana ok. 150 ustaw
- obecnie w Stałym Komitecie Rady Ministrów
- ostatni projekt z 23 maja 2018 r.
- zmiana nazwy na „Ustawa o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679”



Agenda

1. RODO – informacje ogólne
2. Ustawa o ochronie danych osobowych
3. Proces ustawodawczy – UODO
4. D&P – dane kontaktowe

Departament Ochrony Danych Osobowych

1. fachowy audyt i kompleksowe doradztwo
2. merytoryczne przygotowanie administratorów do stosowania RODO
3. reprezentowanie Klientów przed GIODO (wkrótce PUODO)
3. prowadzenie szkoleń w zakresie ODO

DZIĘKUJEMY ZA UWAGĘ.