

I. **Obowiązki administratora**

1. Wprowadzenie **zasady rozliczalności** (ang. accountability), zgodnie z którą administrator danych musi być w stanie wskazać przestrzeganie przepisów i wdrożenie środków.

W związku z wprowadzeniem tej zasady powstają poniższe zmiany:

- a) z dniem 25 maja 2018 przestaje obowiązywać rozporządzenie MSWiA z dn. 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych – rezygnacja z twardych wytycznych dla administratorów i minimalnych standardów technicznych ochrony danych
 - b) każdy administrator samodzielnie dobiera środki ochrony danych osobowych
 - c) administrator będzie musiał faktycznie zapewnić w ten sposób ochronę danych osobowych, samo sporządzenie dokumentacji nie będzie wystarczające
2. Zasady dotyczące ochrony danych osobowych już na etapie projektowania rozwiązań:
 - a) zasada uwzględniania ochrony danych w fazie projektowania (privacy by design)
 - b) domyślna ochrona danych (privacy by default) – analiza zakresu danych pod kątem adekwatności i minimalnego i niezbędnego zakresu
 3. obowiązek prowadzenia **rejestrów czynności** przetwarzania danych osobowych (art. 30 RODO)
 4. administrator przed rozpoczęciem przetwarzania dokonuje **oceny skutków** planowanych operacji przetwarzania dla ochrony danych osobowych (art. 35 RODO)
 5. obowiązek wyznaczenia **inspektorów ochrony danych**, w określonych przypadkach (art. 37 RODO), do zadań inspektora należy:
 - a) informowanie administratora i innych podmiotów o obowiązkach spoczywających na nich z mocy prawa
 - b) monitorowanie przestrzegania prawa
 - c) udzielanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania
 - d) współpraca z organem nadzorczym
 - e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem oraz prowadzenie konsultacji
 6. rozszerzenie obowiązku informacyjnego wobec osób, których dane dotyczą
 7. stosowanie **zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji** może posłużyć za element wywiązania się z

obowiązków przez administratora lub podmiot przetwarzający dane na podstawie umowy powierzenia (art. 40-43 RODO)

8. **zgłaszanie naruszeń** - w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki zgłasza je właściwemu organowi nadzorczemu (art. 33 RODO) a także osobie, której dane dotyczą jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
9. Transfer danych poza UE
10. Bezpośrednia odpowiedzialność przetwarzającego dane – Za naruszenie przepisów RODO dotyczących danych wrażliwych grożą kary w wysokości aż do 20 mln euro lub aż do 4% rocznego światowego obrotu.
11. Ograniczenie profilowania

II. **Prawa osób**

1. Warunki wyrażania zgody – art. 7 RODO
 - a. Administrator musi być w stanie wykazać, że osoba, której dane dotyczą wyraziła zgodę na ich przetwarzanie.
 - b. Jeżeli zgoda wyrażana jest w pisemnym oświadczeniu zawierającym też inne kwestie, zapytanie o zgodę musi nastąpić w sposób wyraźnie odróżniający je od pozostałych kwestii.
 - c. Istnieje możliwość wycofania zgody w dowolnym momencie, z równą łatwością jak udzielenie tej zgody. Musi o tym zostać poinformowana przed wyrażeniem zgody.
 - d. Ocena dobrowolności zgody: jeżeli wyrażenie zgody nie jest niezbędne do wykonania umowy, nie może być od niej uzależnione wykonanie umowy
2. Nowe i rozszerzone prawa obywateli
 - a. Prawo do „bycia zapomnianym” art. 17 RODO
 - b. Prawo do przenoszenia danych art. 20 RODO
 - c. Prawo do sprzeciwu art. 21 RODO