

# COMPLIANCE INSIGHTS

---

Vol. 70

Twoje dane  
„usunięte”... ale  
czy na pewno?  
Backupy i RODO  
w praktyce



# 1. Decyzja, która nie zamyka ryzyka

Z perspektywy zarządu decyzja o usunięciu danych osobowych wydaje się prosta: polecenie zostaje wydane, proces zamknięty. Ryzyko pojawia się później – podczas audytu lub kontroli – gdy okazuje się, że dane nadal znajdują się w kopiach zapasowych.

UODO przypomina, że **backupy są formą przechowywania danych**, a więc stanowią przetwarzanie danych osobowych i **stosuje się do nich wszystkie określone w RODO zasady postępowania z danymi osobowymi.**



## 2. Backup to nie „strefa techniczna”

Kopie zapasowe często funkcjonują poza bieżącym nadzorem zarządczym – jako „obszar techniczny”. To poważne ryzyko.

UODO jednoznacznie wskazuje, że **tworzenie backupów służy realizacji obowiązku zapewnienia bezpieczeństwa danych (art. 32 RODO) poprzez zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, co nie znosi obowiązku respektowania praw osób, których dane dotyczą.**



### 3. Prawo do usunięcia danych osobowych

---

**Prawo do usunięcia danych (art. 17 RODO) musi być realizowane bez zbędnej zwłoki – również w odniesieniu do kopii zapasowych.** Jeżeli żądanie usunięcia danych jest zasadne, administrator powinien usunąć dane ze wszystkich swoich systemów.

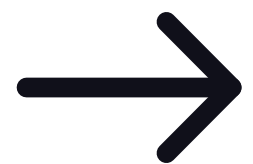
**Brak możliwości technicznej, wysokie koszty lub czasochłonność procesu nie stanowią przesłanki odmowy.** Z punktu widzenia audytu są to sygnały niedostosowania systemów, a nie usprawiedliwienie naruszenia prawa.



## 4. Privacy by design to decyzja biznesowa

UODO akcentuje znaczenie zasady privacy by design jako elementu zarządzania ryzykiem. **Systemy IT – w tym backupy – powinny być zaprojektowane w taki sposób, aby umożliwiały realizację praw osób fizycznych, w tym prawa do usunięcia danych.**

Odpowiedzialność za ten aspekt spoczywa na administratorze danych, który musi wdrożyć odpowiednie środki techniczne i organizacyjne oraz być w stanie wykazać ich skuteczność.



## 5. Wyjątki od prawa do usunięcia danych

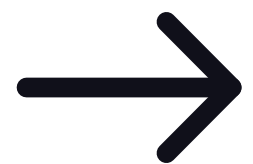
**RODO przewiduje zamknięty katalog wyjątków od prawa do usunięcia danych.** Obejmuje on m.in. konieczność wywiązania się z obowiązków prawnych, interes publiczny czy ustalenie, dochodzenie lub obronę roszczeń.

**Nie obejmuje natomiast argumentów organizacyjnych ani ograniczeń systemowych.** Z perspektywy zarządu oznacza to konieczność świadomej akceptacji ryzyka lub zapewnienia zgodnych z RODO rozwiązań technicznych.



## 6. Koszt zgodności to nie argument obronny

**Jeżeli usunięcie danych bezpośrednio z kopii zapasowej grozi naruszeniem integralności systemu, administrator danych powinien zastosować rozwiązania alternatywne.** Przykładem jest przywrócenie kopii do systemu głównego, usunięcie danych i wykonanie nowego backupu. Proces ten może być czasochłonny, ale pozostaje zgodny z RODO. **Efektywność biznesowa nie może przeważać nad zgodnością prawną. Brak odpowiednich procedur oznacza ryzyko naruszenia przepisów.**



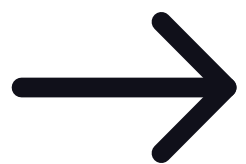
# 7. Zasada rozliczalności

Stanowisko UODO wzmacnia zasadę rozliczalności. **Administrator musi nie tylko działać zgodnie z RODO, ale także być w stanie to wykazać.** W praktyce oznacza to **konieczność posiadania procedur, decyzji i dokumentacji potwierdzających, że prawo do usunięcia danych obejmuje również kopie zapasowe.** Jeżeli wykorzystywany system uniemożliwia realizację tego prawa, problemem jest przyjęte rozwiązanie techniczne, a nie samo żądanie osoby fizycznej.



## 8. Backup jako element governance

Dla organu kierującego działalnością administratora danych jest to sygnał, że obszar backupów nie powinien pozostawać wyłącznie w domenie IT. To **element systemu zarządzania ryzykiem regulacyjnym i compliance**. Procedury realizacji praw osób powinny obejmować również kopie zapasowe. **Brak kontroli nad kopiami zapasowymi może skutkować zarzutem niewdrożenia odpowiednich środków technicznych i organizacyjnych, a w konsekwencji – nawet karami administracyjnymi.**



## 9. Wnioski praktyczne

Wniosek jest jednoznaczny: **prawo do bycia zapomnianym musi być realne, a więc realnie wykonalne w całej architekturze organizacji.**

Backupy nie są neutralnym technicznie detałem, lecz potencjalnym punktem naruszenia RODO.

**Odpowiedzialność za ten obszar spoczywa na administratorze i jego kierownictwie.** Dlatego warto zweryfikować już dziś, czy stosowane rozwiązania backupowe pozwalają spełnić wymogi art. 17 RODO i realizację praw osób fizycznych.



# Kontakt



**Mariusz Purgał**

Partner

[mariusz.purgal@kwkr.pl](mailto:mariusz.purgal@kwkr.pl)



**Alicja Łopacińska**

Associate

[alicja.lopacinska@kwkr.pl](mailto:alicja.lopacinska@kwkr.pl)

## Zespół Compliance KWKR



**Agata  
Baca**



**Katarzyna  
Kanik**



**Justyna  
Staszkiwicz-Maj**



**Anna  
Bartosiak**