WYMAGANA DOKUMENTACJA RODO – CHECKLISTA COMPLIANCE

Jaką dokumentację ochrony danych osobowych powinni mieć agent i broker?

Wielu agentów i brokerów poszukuje informacji, w jaki sposób powinni realizować zgodność z RODO, które stosowane jest już od ponad pięciu lat (od 25 maja 2018 r.). Odpowiedź na to pytanie zależy od kilku czynników, które zostaną przybliżone w niniejszym artykule.

Pierwszym z czynników jest stan spełniania wymogów ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych. RODO nie było bowiem całkowitą rewolucją, szczególnie na polskim rynku, na którym funkcjonuje obecnie dość wysoki standard ochrony praw osób fizycznych. Dlatego w gorszej sytuacji znajdują się podmioty, które do tej pory nie przywiązywały wagi do kwestii ochrony danych osobowych.

W tym przypadku rekomendowane jest rozpoczęcie działań od zbadania, gdzie, z wykorzystaniem jakich narzędzi (systemów) i na jakiej podstawie są przetwarzane dane.

Rekomendowanym krokiem dla każdego podmiotu jest przygotowanie corocznego audytu z wyszczególnieniem stanu procesów i dokumentacji, który da odpowiedź, co i w jaki sposób należy zmienić. W tym miejscu powstaje zwykle pytanie: Czego właściwie nam potrzeba?

Odpowiedzi na to zagadnienie nie udziela niestety samo RODO, które ogranicza się do kilku dokumentów (m.in. rejestru czynności przetwarzania i umowy powierzenia). Aby jednak zrealizować zasady przetwarzania danych osobowych (tj. zgodność z prawem, rzetelność, przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, ograniczenie przechowywania, integralność i poufność, rozliczalność), z pewnością konieczne jest posiadanie szerszego katalogu procedur, instrukcji i wytycznych. Warto zaznaczyć, że nieco inną dokumentację powinien posiadać administrator (zwykle będzie nim broker oraz multiagent), a inną podmiot przetwarzający (zwykle będzie nim agent wyłączny).

Dodatkowo też należy wziąć pod uwagę konieczność implementacji przez branżę ubezpieczeniową unijnego Rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (tzw. DORA), które stosowane będzie od 17 stycznia 2025 r. Już teraz wiele podmiotów wymaga np. obowiązkowych audytów i sformalizowanych zasad dotyczących ciągłości działania oraz wdraża je. Dlatego realizując wdrożenia dla naszych klientów – już dziś uwzględniamy regulację DORA.

Poniżej prezentowany jest rekomendowany zestaw dokumentacji wraz z potencjalnymi skutkami jej braku. Warto pamiętać, że punktem wyjścia dla wszystkich wymienionych poniżej dokumentów winna być przeprowadzona rzetelnie inwentaryzacja i ocena ryzyka. Niestety częstokroć ten element jest pomijany, co powoduje, że dokumenty są nieadekwatne do specyfiki działania danego agenta lub brokera – a co za tym idzie, ich walor przy ewentualnej kontroli jest wątpliwy.

1. **Polityka bezpieczeństwa** – jej brak może stanowić naruszenie art. 24 ust. 1 i 2 RODO (administrator), art. 28 ust. 1 RODO (podmiot przetwarzający).

Konsekwencje: odpowiedzialność odszkodowawcza administratora i podmiotu przetwarzającego z art. 82 RODO, odpowiedzialność administracyjna – do 10 mln euro / 2% światowego obrotu.

2. **Procedura realizacji praw podmiotów danych** – jej brak może stanowić naruszenie art. 24 ust. 1 i 2 RODO w zw. z art. 12-23 RODO (administrator).

Konsekwencje: odpowiedzialność odszkodowawcza administratora z art. 82 RODO, odpowiedzialność administracyjna – do 10 mln euro / 2% światowego obrotu.

3. **Procedura w przypadku naruszenia** – jej brak może stanowić naruszenie art. 32 ust. 1 w zw. z art. 33–34 RODO (administrator oraz podmiot przetwarzający), stanowiąc ryzyko braku odpowiedniej reakcji w przypadku powstania incydentu z zakresu ochrony danych osobowych.

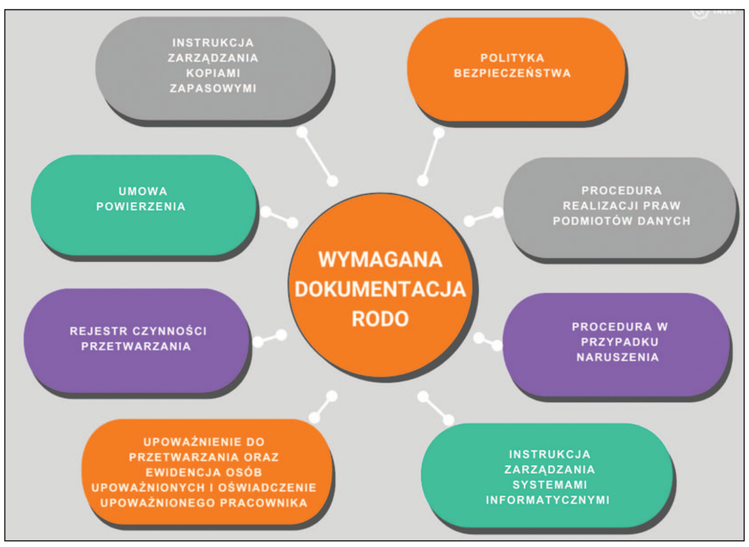
Konsekwencje: odpowiedzialność odszkodowawcza administratora i podmiotu przetwarzającego z art. 82 RODO, odpowiedzialność administracyjna – do 10 mln euro / 2% światowego obrotu.

4. **Instrukcja zarządzania systemami informatycznymi (w przypadku ich posiadania)** – jej brak może stanowić naruszenie art. 32 ust. 1 RODO (administrator oraz podmiot przetwarzający).

Konsekwencje: odpowiedzialność odszkodowawcza administratora i podmiotu przetwarzającego z art. 82 RODO, odpowiedzialność administracyjna – do 10 mln euro / 2% światowego obrotu.

5. **Upoważnienie do przetwarzania dla pracowników/współpracowników oraz ewidencja osób upoważnionych i oświadczenie upoważnionego pracownika** – ich brak może stanowić naruszenie art. 24 ust. 1 w zw. z art. 29 RODO.

Konsekwencje: odpowiedzialność odszkodowawcza administratora i podmiotu przetwarzającego z art. 82 RODO, odpowiedzialność administracyjna – do 10 mln euro / 2% światowego obrotu.



6. **Rejestr czynności przetwarzania** – jego brak będzie stanowił naruszenie art. 30 ust. 1 RODO (administrator), art. 30 ust. 2 RODO (podmiot przetwarzający). Skutki – odpowiedzialność odszkodowawcza administratora i podmiotu przetwarzającego z art. 82 RODO, odpowiedzialność administracyjna – do 10 mln euro / 2% światowego obrotu.

Obowiązek prowadzenia rejestru nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego **mniej niż 250 osób**, chyba że przetwarzanie, którego dokonują, może powodować **ryzyko naruszenia praw lub wolności osób**, których dane dotyczą, **nie ma charakteru sporadycznego** lub obejmuje **szczególne kategorie danych osobowych** lub dane osobowe dotyczące **wyroków skazujących i naruszeń prawa**.

7. **Umowa powierzenia** – jej brak stanowi naruszenie art. 28 ust. 3 RODO (administrator, podmiot przetwarzający podpowierzający przetwarzanie danych osobowych).

Konsekwencje: odpowiedzialność odszkodowawcza administratora i podmiotu przetwarzającego z art. 82 RODO, odpowiedzialność administracyjna – do 10 mln euro / 2% światowego obrotu.

8. **Instrukcja zarządzania kopiami zapasowymi (w przypadku ich tworzenia)** – art. 32 ust. 1 RODO (administrator oraz podmiot przetwarzający).

Konsekwencje: odpowiedzialność odszkodowawcza administratora i podmiotu przetwarzającego z art. 82 RODO, odpowiedzialność administracyjna – do 10 mln euro / 2% światowego obrotu. Jest to oczywiście pewien wycinek obowiązków regulacyjnych dotyczących brokera i agenta ubezpieczeniowego – aby ułatwić „nawigowanie" po różnorodnych obowiązkach, wynikających z wielu aktów prawnych, przygotowaliśmy dla Państwa „Checklistę compliance". Celem budowy tego narzędzia było utworzenie możliwie kompletnej listy obowiązków, jakie ciążą na każdym pośredniku ubezpieczeniowym. Część z nich dotyczy również OFWCA czy wybranych „specjalizacji" branżowych (np. agentów oferujących ubezpieczenia życiowe z opcją inwestycji). Wynikają one z różnych przepisów, dobrych praktyk, komunikatów i innych wytycznych regulatorów. Zbudowana została nie tylko na bazie ogólnodostępnej wiedzy, ale także doświadczeń naszych ekspertów, uczestniczących często w różnych kontrolach czy innych wymianach komunikacji z urzędami (głównie KNF).

r. pr. Tomasz Klemt
Kancelaria Radcy Prawnego
Tomasz Klemt członek Koalicji
na rzecz Zgodności

KOALICJA NA RZECZ ZGODNOŚCI