Lista kontrolna przed kontrolą KRiBSI

Dla firm korzystających z AI w Polsce, IOD i działów compliance. Zaznacz, co już macie; puste pola to zadania.

Dutybound
stan na 23 września 2026 r.

28 października 2026	**min. 7 dni**	**zdalnie**	**14 dni**
kontrole i kary KRiBSI (art. 127 ustawy)	od doręczenia zawiadomienia do kontroli (art. 49 ust. 2)	bez fizycznej obecności stron, z wyjątkami (art. 49 ust. 3–4)	na podpis protokołu lub zastrzeżenia (art. 56 ust. 6)

1. Mieć gotowe przed zawiadomieniem

- [ ] Rejestr systemów AI: nazwa, dostawca, cel, właściciel biznesowy, rola wg AI Act, klasa ryzyka; z odesłaniem do rejestru czynności przetwarzania podstawa pozostałych punktów
- [ ] Wskazane role: kto odpowiada za AI w firmie, kto zatwierdza nowe narzędzia; osoba kontaktowa ds. kontroli i jej zastępca
- [ ] Pisemne zasady korzystania z AI (dozwolone narzędzia, jakie dane wolno wprowadzać) i podpisane oświadczenia pracowników
- [ ] Rejestr szkoleń z AI: kto, kiedy, z jakiego modułu, forma, wynik quizu; program szkolenia art. 4 AI Act, od 2 lutego 2025
- [ ] Sprawdzenie, że żadne zastosowanie nie jest zakazaną praktyką art. 5 AI Act, od 2 lutego 2025
- [ ] Czatboty informują, że są AI; treści syntetyczne i deepfake są oznakowane; zrzuty ekranu z datą art. 50 AI Act, od 2 sierpnia 2026
- [ ] Umowy z dostawcami AI: dokumentacja, zgłaszanie incydentów, wsparcie przejrzystości, dostęp do logów, prawo audytu
- [ ] Procedura reagowania na incydenty AI i rejestr incydentów
- [ ] Spis dokumentów z właścicielem i datą aktualizacji, w jednym miejscu, gotowy do udostępnienia elektronicznie w ciągu godzin
- [ ] Lista materiałów z tajemnicą przedsiębiorstwa, z krótkim uzasadnieniem poufność: art. 50 ust. 8

2. Styk z RODO dla IOD

- [ ] DPIA dla systemów AI, które jej wymagają art. 35 RODO; przy systemach wysokiego ryzyka z informacji od dostawcy art. 26 ust. 9 AI Act
- [ ] Decyzje wyłącznie zautomatyzowane: podstawa i prawa osób art. 22 RODO
- [ ] Czatbot: obok informacji o AI obowiązek informacyjny art. 13 RODO
- [ ] IOD doradza i monitoruje; właścicielem wdrożenia AI jest biznes lub compliance art. 38 ust. 6 RODO

3. Po kontroli

- [ ] Protokół: podpis albo pisemne zastrzeżenia w 14 dni; brak reakcji = odmowa podpisu art. 56 ust. 6 i 8
- [ ] Zalecenia pokontrolne: termin usunięcia co do zasady min. 30 dni; plan z właścicielami art. 57
- [ ] Przegląd po kontroli: o co pytano, czego brakowało, aktualizacja dokumentów

4. Plan na 7 dni po zawiadomieniu

Dzień 0	Zawiadomienie do osoby kontaktowej i prawnika. Zapisz datę doręczenia i zakres z upoważnienia (art. 51).
Dzień 1	Porównaj zakres ze spisem dokumentów, wypisz braki. Ustal techniczną formę kontroli zdalnej.
Dni 2–3	Zbierz dokumenty; sprawdź spójność rejestru, klasyfikacji i umów. Oznacz tajemnicę przedsiębiorstwa.
Dzień 4	Przegląd przez prawnika; przygotuj osoby do rozmów.
Dzień 5	Test połączenia i udostępniania plików; konta tylko do odczytu.
Dzień 6	Zatwierdzenie przez zarząd; protokół spotkań po stronie firmy.
Dzień 7	Kontrola: mówi jedna osoba, prawnik obecny, każde żądanie i przekazany dokument w protokole.

5. Warto wiedzieć

- Kontrolujący może żądać dokumentów, korespondencji e-mail i dostępu do systemów, także w chmurze dostawcy, w zakresie Waszego dostępu art. 52
- Korespondencja z adwokatem lub radcą prawnym jest chroniona art. 54
- Niejasny przepis: opinia indywidualna KRiBSI, 150 zł, 30–60 dni, wiąże organy art. 8–13

Źródła: ustawa z 3 lipca 2026 r. o systemach sztucznej inteligencji (Dz.U. 2026 poz. 1003); rozporządzenie (UE) 2024/1689 (AI Act); RODO. Informacja operacyjna, nie porada prawna.

Kalendarium KRiBSI ze źródłami: getdutybound.com/pl/kribsi/ · Dutybound, ARATIR SYSTEMS P.S.A., Radom