Opinia nr 9/2019 w sprawie projektu wymogów akredytacji podmiotu monitorującego kodeks postępowania zgodnie z art. 41 RODO austriackiego organu nadzorczego ds. ochrony danych

Przyjęta 9 lipca 2019 r.

przyjęte

Spis treści

1 Streszczenie faktów 4
2 Ocena 5
2.1 Ogólne uzasadnienie Rady w odniesieniu do przedłożonego projektu decyzji....5
2.2 Analiza projektu decyzji (składającego się z not wyjaśniających i zarządzenia)....6
2.2.1 NIEZALEŻNOŚĆ....6
2.2.2 KONFLIKT INTERESÓW....8
2.2.3 WIEDZA EKSPERCKA....9
2.2.4 USTANOWIONE PROCEDURY I STRUKTURY....9
2.2.5 PRZEJRZYSTE ROZPATRYWANIE SKARG....10
2.2.6 KOMUNIKACJA Z WŁAŚCIWYM ORGANEM NADZORCZYM....11
2.2.7 MECHANIZMY PRZEGLĄDU....12
2.2.8 STATUS PRAWNY....12
3 Wnioski/Zalecenia....13
4 Uwagi końcowe....15

Europejska Rada Ochrony Danych

Uwzględniając art. 63 i 64 ust. 1 lit. c), ust. 3-8 oraz art. 41 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO”),

uwzględniając Porozumienie EOG, a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.,

uwzględniając art. 10 i 22 swojego regulaminu wewnętrznego z dnia 25 maja 2018 r., zmienionego w dniu 23 listopada 2018 r.,

a także mając na uwadze, co następuje:

(1) Główną rolą Europejskiej Rady Ochrony Danych (zwaną dalej „Radą”) jest zapewnienie spójnego stosowania RODO w przypadku, gdy organ nadzorczy (ON) zamierza zatwierdzić wymogi akredytacji podmiotu monitorującego kodeks postępowania (zwanego dalej „kodeksem”) zgodnie z art. 41. W związku z powyższym celem niniejszej opinii jest przyczynienie się do zharmonizowania podejścia w odniesieniu do sugerowanych wymogów, które organ nadzorczy ds. ochrony danych powinien opracować i które mają zastosowanie podczas akredytacji podmiotu monitorującego kodeks przez właściwy organ nadzorczy. Nawet jeżeli RODO bezpośrednio nie nakłada określonych wymogów akredytacji, sprzyja to spójności. Rada dąży do osiągnięcia tego celu w swojej opinii poprzez: po pierwsze, wnioskowanie do właściwych organów nadzorczych o sporządzenie projektu kryteriów akredytacji podmiotów monitorujących w oparciu o „Wytyczne 1/2019 w sprawie kodeksów postępowania i podmiotów monitorujących na mocy rozporządzenia 2016/679” (zwane dalej „wytycznymi”), z wykorzystaniem ośmiu wymogów określonych w wytycznych w sekcji o akredytacji (sekcja 12); po drugie, przedstawienie pisemnych wytycznych wyjaśniających wymogi akredytacji; oraz zwrócenie się do nich o przyjęcie tych wymogów zgodnie z niniejszą opinią, tak aby osiągnąć zharmonizowane podejście.

(2) W odniesieniu do art. 41 RODO właściwe organy nadzorcze powinny przyjąć wymogi akredytacji podmiotów monitorujących zatwierdzone kodeksy. Powinny jednak stosować mechanizm spójności w celu umożliwienia określenia odpowiednich wymogów gwarantujących monitorowanie przez podmioty monitorujące przestrzegania kodeksów w sposób kompetentny, spójny i niezależny, ułatwiając tym samym właściwe wdrażanie kodeksów w całej Unii, a w rezultacie przyczyniając się do właściwego stosowania RODO.

(3) W celu zatwierdzenia kodeksu obejmującego organy niepubliczne i podmioty, podmiot monitorujący (lub podmioty) musi być zidentyfikowany jako część kodeksu i akredytowany przez właściwy organ nadzorczy jako zdolny do skutecznego monitorowania kodeksu. W RODO nie uwzględniono definicji akredytacji. Jednakże art. 41 ust. 2 RODO określa ogólne wymogi akredytacji

podmiotu monitorującego. Istnieje szereg wymogów, które należy wykazać w sposób satysfakcjonujący dla właściwego organu nadzorczego w zakresie akredytacji podmiotu monitorującego. Aby uzyskać akredytację, twórcy kodeksów są zobowiązani do wyjaśnienia i wykazania, w jaki sposób proponowany przez nich podmiot monitorujący spełnia wymogi określone w art. 41 ust. 2.

(4) Podczas gdy wymogi akredytacji podmiotów monitorujących podlegają mechanizmowi spójności, rozwój wymogów akredytacji przewidzianych w wytycznych powinien uwzględniać sektor lub specyfikę kodeksu. Właściwe organy nadzorcze mają swobodę uznania w odniesieniu do zakresu stosowania i specyfiki każdego kodeksu i powinny uwzględniać istotne prawodawstwo. W związku z powyższym celem opinii Rady jest uniknięcie istotnych niespójności, które mogą mieć wpływ na działanie podmiotów monitorujących, a w konsekwencji na reputację kodeksów postępowania RODO i ich podmiotów monitorujących.

(5) W tym względzie wytyczne przyjęte przez Radę posłużą jako nić prowadząca w kontekście mechanizmu spójności. W szczególności w wytycznych Rada wyjaśniła, że nawet jeżeli akredytacja podmiotu monitorującego ma zastosowanie wyłącznie do konkretnego kodeksu, podmiot monitorujący może być akredytowany w odniesieniu do więcej niż jednego kodeksu, pod warunkiem, że spełnia on kryteria akredytacji dla każdego kodeksu.

(6) Opinię Rady należy przyjąć zgodnie z art. 64 ust. 3 RODO w związku z art. 10 ust. 2 regulaminu wewnętrznego EROD w terminie ośmiu tygodni od pierwszego dnia roboczego po podjęciu przez Radę i właściwy organ nadzorczy decyzji o kompletności akt. Na mocy decyzji Rady, ze względu na złożony charakter sprawy termin ten może zostać przedłużony o sześć tygodni.

PRZYJMUJE OPINIĘ:

1 STRESZCZENIE FAKTÓW

1. Austriacki organ nadzorczy (AT ON) przedłożył Radzie projekt decyzji zawierający wymogi akredytacji wobec podmiotu monitorującego kodeks postępowania za pośrednictwem systemu IMI, zwracając się do Rady o wydanie opinii zgodnie z art. 64 ust. 1 lit. c) w celu wypracowania spójnego podejścia na poziomie Unii. Decyzja w sprawie kompletności akt została podjęta 9 kwietnia 2019 r.

2. Projekt wymogów akredytacji dla podmiotów monitorujących kodeks został przedstawiony przez AT ON w wersji angielskiej, chociaż pierwotnie był on sporządzony w języku niemieckim. Rada niniejszym wydaje opinię o angielskiej wersji projektu wymogów akredytacji, zalecając AT ON zmianę i dostosowanie obu wersji zgodnie z niniejszą opinią.

3. Zgodnie z art. 10 ust. 2 regulaminu wewnętrznego Rady[1], ze względu na złożoność rozpatrywanej sprawy, Rada zdecydowała o przedłużeniu początkowego ośmiotygodniowego okresu o kolejne sześć tygodni, do 16 lipca 2019 r.

2 OCENA

2.1 Ogólne uzasadnienie Rady w odniesieniu do przedłożonego projektu decyzji

4. Wszystkie wymogi akredytacji przedłożone Radzie w celu uzyskania opinii muszą w pełni odnosić się do wymogów art. 41 ust. 2 RODO i być zgodne z ośmioma obszarami określonymi przez Radę w sekcji o akredytacji wytycznych (sekcja 12, str. 21-25). Opinia Rady ma na celu zapewnienie spójności i prawidłowego stosowania art. 41 ust. 2 RODO w odniesieniu do przedstawionego projektu.

5. Oznacza to, że przy opracowywaniu wymogów akredytacji podmiotu monitorującego kodeksy zgodnie z art. 41 ust. 3 i art. 57 ust. 1 lit. p) RODO, wszystkie ON będą spełniały te podstawowe wymogi przewidziane w wytycznych, a Rada zaleci ON wprowadzenie odpowiednich zmian w swoich projektach w celu zapewnienia spójności.

6. Wszystkie kodeksy obejmujące organy niepubliczne i podmioty muszą posiadać akredytowane podmioty monitorujące. W RODO wyraźnie wskazano, że organy nadzorcze, Rada i Komisja „zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu niniejszego rozporządzenia — z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.” (artykuł 40 ust. 1 RODO). W związku z powyższym Rada uznaje, że wymogi muszą być stosowane do różnych rodzajów kodeksów, mających zastosowanie do sektorów o różnej wielkości, uwzględniających różne interesy i obejmujących czynności związane z przetwarzaniem o różnych poziomach ryzyka.

7. W niektórych obszarach Rada wesprze rozwój zharmonizowanych wymogów zachęcając ON do rozważenia przedstawionych przykładów wyłącznie w celach ilustracyjnych. W związku z powyższym zachęty i przykłady przedstawione w niniejszej opinii nie muszą być stosowane. Celem tych przykładów jest pomoc AT ON w dalszym rozwijaniu spójnych wymogów akredytacji zgodnie z niniejszą opinią.

8. W przypadku gdy niniejsza opinia nie dotyczy konkretnego wymogu, oznacza to, że Rada nie zwraca się do AT ON o podjęcie dalszych działań.

9. Rada podkreśla, że dokument przedłożony przez AT ON jest projektem decyzji dotyczącym wymogów akredytacji dla podmiotów monitorujących, składającym się z dwóch części:

    1) „Uwagi wyjaśniające”, które zawierają ogólne i szczegółowe wyjaśnienia.

    2) „Zarządzenie”, które określa wymogi akredytacji AT.

[1] Wersja 2, ostatnio zmieniona i przyjęta dnia 23 listopada 2018 r.

10. Niniejsza opinia nie dotyczy pozycji przedłożonych przez AT ON, które są poza zakresem art. 41 ust. 2 RODO, takich jak odniesienia do prawodawstwa krajowego. Rada zauważa jednak, że prawodawstwo krajowe powinno być zgodne z RODO, jeżeli jest to wymagane.

2.2 Analiza projektu decyzji (składającego się z not wyjaśniających i zarządzenia)

11. Biorąc pod uwagę, że:

    a. Artykuł 57 ust. 1 lit. p) i lit. q) RODO stanowi, że właściwy organ nadzorczy opracowuje i publikuje wymogi akredytacji podmiotów monitorujących oraz przeprowadza akredytację;
    b. Artykuł 41 ust. 4 RODO wymaga, aby wszystkie kodeksy (z wyjątkiem kodeksów obejmujących organy publiczne zgodnie z art. 41 ust. 6) posiadały akredytowany podmiot monitorujący; oraz
    c. Artykuł 41 ust. 2 RODO zawiera wykaz obszarów akredytacji, które muszą zostać objęte działaniami podmiotu monitorującego, aby uzyskać akredytację,

    Rada jest zdania, że:

2.2.1 NIEZALEŻNOŚĆ

12. W odniesieniu do sekcji trzeciej zarządzenia AT ON Rada podkreśla, że obowiązek dostarczenia dowodów dotyczących niezależności podmiotu monitorującego spoczywa na podmiocie ubiegającym się o akredytację [zob. art. 41 ust. 2 lit. a) RODO]. Rada zaleca, aby zostało to wyjaśnione w wymogach AT ON.

13. Rada zauważa, że noty wyjaśniające AT ON, sekcja „uwagi ogólne" dotycząca wymogów, odnoszą się do niezależności „w odniesieniu do charakteru kodeksu". Wytyczne zawierają dalsze informacje na temat tego, co to oznacza, tj. należy wykazać niezależność danego podmiotu w odniesieniu do członków kodeksu, zawodu, branży lub sektora, do których kodeks ma zastosowanie oraz samego właściciela kodeksu. W związku z powyższym Rada zaleca, aby AT ON przeredagował to odniesienie zgodnie z wytycznymi.

14. Rada wyraża opinię, że niezależność podmiotu monitorującego należy rozumieć jako szereg formalnych zasad i procedur powoływania, zakresu uprawnień i funkcjonowania podmiotu monitorującego. Te zasady i procedury umożliwią podmiotowi monitorującemu przeprowadzenie monitorowania zgodności z kodeksem postępowania w sposób całkowicie autonomiczny, bez bezpośredniego lub pośredniego wpływu, ani też niepodlegający żadnej formie presji, która mogłaby mieć wpływ na jego decyzje. Oznacza to, że podmiot monitorujący nie powinien otrzymywać żadnych instrukcji dotyczących wykonywania swoich zadań od członków kodeksu, zawodu, branży lub sektora, do których kodeks ma zastosowanie, ani też od samego właściciela kodeksu.

15. W przypadku gdy podmiot monitorujący stanowi część organizacji właściciela kodeksu, należy zwrócić szczególną uwagę na zdolność podmiotu do niezależnego działania. Przykłady wewnętrznych podmiotów monitorujących mogą obejmować wewnętrzny komitet *ad hoc* lub odrębny departament

w ramach organizacji właściciela kodeksu. Należy ustanowić zasady i procedury w celu zapewnienia, aby taki „komitet" działał niezależnie i bez jakiejkolwiek presji ze strony właściciela kodeksu lub członków kodeksu.

16. Rada podkreśla, że wymogi AT ON nie odnoszą się do dwóch głównych modeli monitorowania określonych w wytycznych. W związku z powyższym Rada zaleca, aby AT ON zmienił wymogi w celu odzwierciedlenia tej elastyczności. Jednym z wariantów byłoby wymaganie, aby wewnętrzny podmiot monitorujący przedstawił dowód istnienia dodatkowych środków w celu zagwarantowania, że związek z podmiotem prawnym (którego częścią jest podmiot monitorujący) nie naraża na szwank niezależności jego czynności monitorujących.

17. Rada zauważa, że przepis szczegółowy projektu wymogów akredytacji przedłożonego przez AT ON jest poświęcony wykazaniu niezależności przez podmiot monitorujący (sekcja 3.2 zarządzenia AT). Wymieniony przepis wymaga informacji o osobach upoważnionych do podejmowania decyzji, wykazując, że nie istnieją osobiste powiązania z monitorowanymi podmiotami. Ponadto w nocie wyjaśniającej dotyczącej wymogów w zakresie niezależności wyjaśnia się, że podmiot monitorujący nie może być prawnie, gospodarczo, osobiście lub zawodowo podporządkowany monitorowanym podmiotom lub pozostawać w ścisłym związku z nimi, co mogłoby podważyć jego osąd lub jego niezależność i uczciwość podczas pełnienia funkcji podmiotu monitorującego.

18. Rada wyraża opinię, że wymogi akredytacji powinny zdefiniować niezależność i jasno określać obszary, w których podmiot monitorujący powinien wykazywać niezależność. W tym względzie Rada zaleca, aby AT SA dalej wzmacniał sekcję dotyczącą niezależności zgodnie z czterema obszarami omówionymi poniżej.

1) PROCEDURY PRAWNE I DECYZYJNE

19. Forma prawna i organizacja podmiotu monitorującego musi chronić podmiot monitorujący przed bezprawnym naciskiem ze strony członków kodeksu lub właściciela kodeksu, który mógłby mieć wpływ na monitorowanie zgodności kodeksu. Przykładowo czas trwania lub wygaśnięcie mandatu podmiotu monitorującego należy ustalić w taki sposób, aby uniknąć nadmiernego uzależnienia od przedłużenia lub obawy przed utratą powołania, w zakresie, który negatywnie wpływa na niezależność prowadzenia czynności monitorujących przez podmiot monitorujący.

20. Procedura decyzyjna określona przez podmiot monitorujący musi również zachować jego autonomię i niezależność. Przykładowo podmiot monitorujący musi być niezależny podczas podejmowania decyzji oraz stosowania sankcji wobec administratora lub podmiotu przetwarzającego zgodnie z kodeksem.

2) FINANSOWY

21. Podmiotom monitorującym należy zapewnić stabilność finansową i zasoby niezbędne do skutecznego wykonywania swoich zadań, jak również możliwość niezależnego zarządzania swoim budżetem. Środki, za pomocą których podmiot monitorujący uzyskuje wsparcie finansowe (np. opłata wnoszona przez członków kodeksu postępowania), nie powinny negatywnie wpływać na niezależność jego zadania zapewnienia monitorowania zgodności kodeksu.

22. Przykładowo podmiot monitorujący nie powinien być uznawany jako niezależny finansowo, jeżeli zasady regulujące jego wsparcie finansowe umożliwiają członkowi kodeksu, wobec którego kontrolę prowadzi podmiot monitorujący, wstrzymanie wnoszenia do niego wkładów finansowych w celu uniknięcia ewentualnej sankcji ze strony podmiotu monitorującego.

3) ORGANIZACYJNY

23. Podmioty monitorujące powinny dysponować zasobami ludzkimi i technicznymi niezbędnymi dla skutecznego wykonywania swoich zadań. Podmioty monitorujące powinny składać się z odpowiedniej liczby pracowników, tak aby były w stanie w pełni realizować funkcje monitorujące, odzwierciedlające dany sektor i ryzyko związane z przetwarzaniem, do którego odnosi się kodeks postępowania. Personel podmiotu monitorującego jest odpowiedzialny i zachowuje uprawnienia do podejmowania decyzji dotyczących czynności monitorowania. Te organizacyjne aspekty można wykazać poprzez procedurę powoływania pracowników podmiotu monitorującego, wynagrodzenie tych pracowników, jak również czas trwania mandatu, umowy lub innej formalnej umowy z podmiotem monitorującym.

4) ROZLICZALNOŚĆ

24. Podmiot monitorujący powinien być w stanie wykazać „rozliczalność" swoich decyzji i podjętych czynności w celu uznania go za niezależny. Można to osiągnąć dzięki m.in. określeniu ról i struktury podejmowania decyzji oraz procedur sprawozdawczych.

2.2.2 KONFLIKT INTERESÓW

25. Rada zauważa, że wymogi akredytacji AT ON nie odnoszą się do konfliktów interesów. Rada zaleca, aby AT ON dodał kryteria dotyczące procedur unikania konfliktu interesów. Takie procedury mogą obejmować podejście oparte na analizie ryzyka i będą różnić się w zależności od kodeksu. Ryzyko może wynikać z czynności lub związków między podmiotem monitorującym a jego pracownikami.

26. Przykładem konfliktu interesów mogą być pracownicy podmiotu monitorującego rozpatrujący skargi przeciwko organizacji, dla której pracują. W celu uniknięcia konfliktu interesów pracownicy deklarowaliby takie okoliczności, a praca zostałaby przekazana.

27. Rada zachęca AT ON do rozważenia następujących praktycznych przykładów wymogów akredytacji:

- Podmiot monitorujący określa sytuacje, które mogą prowadzić do powstania konfliktu interesów (z powodów jego pracowników, struktury, procedur, itp.) i ustanawia wewnętrzne zasady w celu uniknięcia konfliktów interesów.
- Podmiot monitorujący zapewnia procedurę postępowania ze skutkami sytuacji określanych jako mogące powodować konflikt interesów.
- Pracownik podmiotu monitorującego musi zobowiązać się na piśmie do przestrzegania tego wymogu oraz do zgłaszania wszelkich sytuacji mogących powodować konflikt interesów i do przestrzegania procedur w celu uniknięcia takich konfliktów.

- Podmiot monitorujący na bieżąco określa i eliminuje ryzyko wobec swojej bezstronności. Dowody będą obejmować podejście do zarządzania ryzykiem i związane z nim procedury.

2.2.3 WIEDZA EKSPERCKA

28. Rada zwraca uwagę, że wymogi AT ON w zakresie wiedzy fachowej obejmują: doskonałą znajomość zagadnień ochrony danych, jak również odpowiedni stopień (lub równoważne kwalifikacje), lub co najmniej pięć lat odpowiedniego doświadczenia w sektorze, co może obejmować maksymalnie dwa lata działalności zawodowej w dziedzinie innej niż przedmiot kodeksu (sekcje 3.4 i 3.5 zarządzenia AT).

29. Rada przyznaje, że wytyczne wyznaczają wysokie wymagania wobec podmiotów monitorujących w zakresie wiedzy fachowej obejmującej: dogłębne zrozumienie kwestii związanych z ochroną danych, znajomość konkretnych czynności przetwarzania w odniesieniu do kodeksu oraz odpowiednie doświadczenie operacyjne i szkolenia w zakresie monitorowania, takie jak audyt.

30. Rada uważa, że wymogi akredytacyjne muszą być przejrzyste. Muszą także zapewnić podmiotom monitorującym ubiegającym się o akredytację w odniesieniu do kodeksów obejmujących czynności przetwarzania mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (art. 40 ust. 1 RODO).

31. Zgodnie z wymaganiami wytycznych każdy kodeks musi spełniać kryteria mechanizmu monitorowania (w sekcji 6.4 wytycznych), wykazując „dlaczego ich propozycje związane z monitorowaniem są odpowiednie i możliwe do wykonania z operacyjnego punktu widzenia" (pkt 41, s. 17 wytycznych). W tym kontekście wszystkie kodeksy z podmiotami monitorującymi będą musiały wyjaśniać niezbędny poziom wiedzy fachowej wobec podmiotów monitorujących w celu skutecznego prowadzenia działań monitorujących kodeks. To może obejmować uwzględnienie takich czynników, jak: wielkość danego sektora, różnorodność interesów oraz ryzyko wynikające z czynności przetwarzania, do których odnosi się kodeks. Pozostaje to bez szkody dla wymogów ochrony danych. Byłoby to również istotne, jeżeli istniałoby kilka podmiotów monitorujących, ponieważ kodeks pomoże zapewnić jednolite stosowanie wymogów w zakresie wiedzy fachowej przez wszystkie podmioty monitorujące obejmujące ten sam kodeks.

32. Rada zachęca AT ON do uwzględnienia dodatkowych wymogów w zakresie wiedzy fachowej, które mogą być określone w kodeksie oraz do zapewnienia, że wiedza specjalistyczna każdego podmiotu monitorującego jest oceniana zgodnie z danym kodeksem. Wtedy ON sprawdzi, czy podmiot monitorujący posiada odpowiednie kompetencje w zakresie konkretnych obowiązków i odpowiedzialności, aby podjąć się skutecznego monitorowania kodeksu.

2.2.4 USTANOWIONE PROCEDURY I STRUKTURY

33. Rada zauważa, że sekcja 4 zarządzenia jest zbyt ogólna. Rada jest zdania, że procedury monitorowania zgodności z kodeksami postępowania muszą być odpowiednio szczegółowe, aby zapewnić spójną realizację obowiązków podmiotów monitorujących kodeks.

34. Procedury muszą obejmować cały proces monitorowania, od przygotowania oceny do zakończenia audytu i dodatkowych narzędzia, aby zapewnić, że odpowiednie czynności zostały podjęte w celu usunięcia skutków naruszeń i zapobieżenia powtarzającym się wykroczeniom.

35. Podmiot monitorujący powinien przedstawić dowody potwierdzające istnienie wstępnych, doraźnych i regularnych procedur monitorowania przestrzegania przez członków kodeksów postępowania w jasno określonych ramach czasowych oraz sprawdzić kwalifikacje członków zanim przystąpią do kodeksu.

36. Ponadto personel podmiotu monitorującego zachowuje poufność wszystkich informacji uzyskanych czy utworzonych w trakcie wykonywania czynności monitorowania, z wyjątkiem sytuacji wymaganych przez prawo.

37. Rada zachęca AT ON do rozważenia następujących przykładów procedur:

- Procedura zapewniająca plany audytów, które mają być przeprowadzane w określonym przedziale czasowym (kontrola wstępna i kontrole powtarzalne), w oparciu o kryteria takie jak liczba podmiotów przestrzegających kodeks postępowania, zakres geograficzny, otrzymane skargi, itp.
- Procedura audytu określająca metodologię audytu, która ma mieć zastosowanie, tj. zestaw kryteriów, które mają być ocenione (wspólna siatka oceny), rodzaj audytu (samoocena, audyty poza terenem lub na miejscu, normy audytu ISO), dokumentacja ustaleń, itp.
- Procedura badania, identyfikacji i zarządzania przypadkami naruszenia przepisów kodeksu, która pozwala na zastosowanie, w razie potrzeby, sankcji określonych w kodeksie postępowania (matryca sankcji)

38. Rada zaleca, aby opcjonalne wymogi dotyczące procedur monitorowania zostały przedstawione w notach wyjaśniających AT oraz aby obowiązkowe wymogi zostały wyjaśnione w zarządzeniu AT.

39. Rada zaleca, aby cele dla każdej wymaganej procedury były wyraźnie określone w wymogach akredytacji.

40. Rada zaleca wyjaśnienie odwołania do „odpowiednich certyfikatów", które występuje więcej niż raz w projekcie wymogów akredytacji AT.

2.2.5 PRZEJRZYSTE ROZPATRYWANIE SKARG

41. W odniesieniu do procedury rozpatrywania skarg Rada zauważa, że kryteria akredytacji AT ON (sekcja 5.3.4 zarządzenia AT ON) obejmują czas trwania postępowania, stwierdzając, że „w żadnym przypadku nie powinien on przekroczyć dwóch miesięcy od daty otrzymania skargi".

42. Rada zaleca, aby wymogi dotyczące procesu rozpatrywania skarg zostały ustalone na wysokim poziomie i by wyznaczyć rozsądne ramy czasowe na udzielenie odpowiedzi na skargi. Przykładem rozsądnego terminu może być powiadomienie skarżącego w ciągu trzech miesięcy o postępach lub wynikach rozpatrywania skargi (podobnie jak w art. 78 ust. 2 RODO). Proces powinien być:

udokumentowany, niezależny, skuteczny i przejrzysty, aby zapewnić zaufanie do kodeksu. Dostępne procedury składania skarg powinny być ujęte w samym kodeksie. Proces rozpatrywania skarg powinien być łatwo dostępny dla osób, których dane dotyczą, oraz dla społeczności.

43. Rada zachęca AT ON do rozważenia następujących przykładów wymogów:

- Podmiot monitorujący przedstawia dowody potwierdzające sposób, w jaki będzie zarządzał procedurami rozpatrywania skarg i wyjaśniał ramy czasowe.
- Podmiot monitorujący stworzy zarys procedury przyjmowania, zarządzania i rozpatrywania skarg. Omawiana procedura musi być niezależna i przejrzysta.
- Omawiana procedura skargi jest łatwo i ogólnie dostępna.
- Omawiana procedura zapewnia rozpatrzenie wszystkich skarg w rozsądnym terminie.
- Podmiot monitorujący prowadzi dokumentację wszystkich otrzymanych skarg i podjętych działań, do której ON ma nieograniczony dostęp.

2.2.6 KOMUNIKACJA Z WŁAŚCIWYM ORGANEM NADZORCZYM

44. Rada podkreśla, że zarządzenie AT ON, sekcja 6.4 przewiduje składanie corocznych sprawozdań przez podmiot monitorujący właściwemu organowi nadzorczemu (zwanemu dalej „właściwym ON"). Rada zaleca, aby AT ON zmienił sekcję 6.4 zarządzenia w celu zapewnienia bardziej regularnej komunikacji z właściwym ON w ciągu roku.

45. Rada jest zdania, że wymogi muszą odnosić się do takich obszarów jak: działania podjęte w przypadku naruszenia kodeksu i przyczyny ich podjęcia (art. 41 ust. 4 RODO), sprawozdania okresowe, przeglądy lub wyniki audytu. Kodeks sam w sobie określa także wymogi w zakresie komunikacji z właściwym ON, w tym odpowiednie doraźne i okresowe sprawozdania. Właściwy ON powinien zostać bezzwłocznie poinformowany w przypadku poważnych naruszeń kodeksu przez członków kodeksu prowadzących do poważnych działań takich jak zawieszenie lub wykluczenie z kodeksu.

46. Rada stwierdza, że „istotna zmiana" obejmuje wszelkie zmiany, które mają wpływ na zdolność podmiotu monitorującego do niezależnego i skutecznego pełnienia swojej funkcji. Istotna zmiana spowodowałaby konieczność przeprowadzenia ponownej akredytacji lub nowego procesu akredytacji. Rada zaleca, aby AT ON zajął się zgłaszaniem wszelkich istotnych zmian do właściwego ON w kryteriach akredytacji.

47. Rada zachęca AT ON do rozważenia następujących przykładów kryteriów:

- Podmiot monitorujący ustanawia mechanizmy sprawozdawczości.
- Podmiot monitorujący bez zbędnej zwłoki informuje właściwy ON o wszelkich istotnych zmianach w podmiocie monitorującym (w szczególności dotyczących struktury lub organizacji), które mogą

podważyć niezależność, wiedzę fachową i brak jakiegokolwiek konfliktu interesów lub negatywnie wpłynąć na jego działalność.

2.2.7 MECHANIZMY PRZEGLĄDU

48. Rada jest zdania, że podmiot monitorujący odgrywa kluczową rolę w przyczynianiu się do przeglądu kodeksu i wprowadza aktualizacje do niego (zmianę lub rozszerzenie kodeksu) zgodnie z decyzją właściciela kodeksu.

49. Rada zachęca do stosowania wymogów akredytacji, które wymagają od podmiotu monitorującego opracowania mechanizmów umożliwiających przekazywanie informacji zwrotnych właścicielom kodeksu. Niektóre opcje dotyczą wykorzystania wyników procesu audytu, rozpatrywania skarg i czynności podjętych w sprawach o naruszenie kodeksu.

50. Dla przykładu, dokumentacja rozpatrywania skarg (otrzymanych i rozpatrzonych), naruszeń i środków ochrony prawnej mogą być dobrym sposobem na scentralizowanie odpowiednich informacji w celu udoskonalenia kodeksu.

51. Rada zachęca AT ON do zapewnienia wymogów akredytacji gwarantujących, że podmiot monitorujący przyczyni się do przeglądu kodeksu, zgodnie z instrukcjami właściciela kodeksu.

2.2.8 STATUS PRAWNY

52. Rada zauważa, że sekcja 2.2 zarządzenia AT ON stanowi, że podmiot monitorujący może mieć siedzibę poza terenem EOG. Rada jest zdania, że podmiot monitorujący wymaga posiadania jednostki organizacyjnej na terenie EOG. Ma to na celu zapewnienie, że może on przestrzegać praw osoby, której dane dotyczą, rozpatrywać skargi oraz że RODO jest wykonalne, a także zapewnia nadzór ze strony właściwego ON. Rada zaleca, aby AT ON wymagał od podmiotu monitorującego posiadania jednostki organizacyjnej na terenie EOG.

53. Ponadto Rada podkreśla, że projekt wymogów AT ON nie przewiduje akredytacji podmiotów monitorujących w odniesieniu do kodeksów, które zostały zatwierdzone jako narzędzie międzynarodowego przekazywania danych wraz z wiążącymi i możliwymi do wyegzekwowania zobowiązaniami administratora danych lub podmiotu przetwarzającego w państwie trzecim w celu stosowania odpowiednich zabezpieczeń (art. 46 ust. 2 lit. e) RODO). W tym względzie warto zauważyć, że może zaistnieć potrzeba dodania dodatkowych wymogów po przyjęciu przez Radę wytycznych dotyczących kodeksów jako środka ułatwiającego międzynarodowe przekazywanie danych.

54. Rada zauważa, że w nocie wyjaśniającej AT ON do sekcji 2.1 wyjaśniono, że osoby fizyczne mogą być akredytowane jako podmiot monitorujący. Rada zachęca AT ON do przedstawienia dodatkowych wymogów w celu akredytacji takiego podmiotu monitorującego. Obejmowałyby one: możliwość wykazania dostępności odpowiednich zasobów na realizację konkretnych zadań oraz obowiązków, jak

również pełne funkcjonowanie mechanizmu monitorowania w czasie. Przykłady scenariuszy do rozważenia obejmują: przypadki rezygnacji lub czasowej niezdolności danej osoby.

55. Rada zaleca, aby AT ON wymagał od podmiotu monitorującego dostępu do odpowiednich zasobów wymaganych do wypełnienia swoich obowiązków związanych z monitorowaniem, w szczególności w odniesieniu do akredytacji osoby fizycznej jako podmiotu monitorującego.

56. Ponadto sam kodeks postępowania musi dowodzić, że funkcjonowanie mechanizmu monitorowania kodeksu jest trwałe w czasie i obejmuje najgorsze scenariusze, takie jak niezdolność do pełnienia funkcji monitorującej. W tym względzie wskazane jest wprowadzenie wymogu, aby podmiot monitorujący wykazywał, że jest w stanie zapewnić mechanizm monitorujący kodeks postępowania przez odpowiedni okres. W związku z powyższym Rada zaleca, aby AT ON wyraźnie wymagał od podmiotów monitorujących wykazania ciągłości funkcji monitorowania w czasie.

57. Rada jest zdania, że podmiot monitorujący nie musi posiadać specjalnej formy prawnej, aby ubiegać się o akredytację pod warunkiem, że może ponosić odpowiedzialność za wszystkie swoje czynności monitorowania i wykaże wystarczające zasoby do realizacji swoich funkcji monitorowania (np. skuteczność administracyjnych kar pieniężnych, itp.)

58. Wreszcie Rada podkreśla, że noty wyjaśniające i zarządzenie AT ON nie odnoszą się do umów o podwykonawstwo, pozostawiając ten obszar otwarty do podejmowania decyzji przez podmioty monitorujące ubiegające się o akredytację. Rada zaleca, aby AT ON wyjaśnił, czy podmiot monitorujący może odwoływać się do podwykonawców oraz na jakich warunkach i czy są one odzwierciedlone odpowiednio w notach wyjaśniających lub w zarządzeniu. Jeżeli AT ON wskazuje, że podwykonawstwo jest dozwolone, Rada zaleca, aby AT ON wskazał w swoim zarządzeniu, że obowiązki mające zastosowanie do podmiotu monitorującego mają zastosowanie w ten sam sposób do podwykonawców.

3 WNIOSKI/ZALECENIA

59. Projekt wymogów akredytacji austriackiego organu nadzorczego może prowadzić do niespójnego stosowania akredytacji podmiotów monitorujących i konieczne jest wprowadzenie następujących zmian:

60. W odniesieniu do „niezależności” Rada zaleca, aby AT ON:

1. wyjaśnił, że zadanie dostarczenia dowodów dotyczących niezależności podmiotu monitorującego w stopniu zadowalającym dla właściwego ON spoczywa na podmiocie ubiegającym się o akredytację;

2. przeredagował notę wyjaśniającą „w odniesieniu do przedmiotu kodeksu”, tak aby była ona zgodna z wytycznymi;

3. zmienił wymogi w celu odzwierciedlenia dwóch modeli podmiotów monitorujących określonych w wytycznych; oraz

4. wzmocnił wymogi zgodnie z czterema obszarami (prawnym i podejmowania decyzji, finansowym, organizacyjnym i odpowiedzialności) w celu zdefiniowania niezależności.

61. W odniesieniu do „konfliktu interesów” Rada zaleca, aby AT ON:

1. dodał wymogi dotyczące procedur w celu uniknięcia konfliktu interesów.

62. W odniesieniu do „ustalonych procedur i struktur” Rada zaleca, aby AT ON:

1. zapewnił opcjonalne wymogi dotyczące procedur monitorowania w notach wyjaśniających AT i wyjaśnił obowiązkowe wymogi w zarządzeniu AT;

2. wyraźnie określił cele każdej wymaganej procedury w wymogach akredytacji; oraz

3. wyjaśnił odniesienia do „odpowiednich certyfikatów” — które występują więcej niż raz w projekcie AT dotyczącym wymogów akredytacji.

63. W odniesieniu do „przejrzystego rozpatrywania skarg” Rada zaleca, aby AT ON:

1. wymagał, aby procedury rozpatrywania skarg były ustalane na wysokim poziomie i ustanawiał rozsądne ramy czasowe na udzielenie odpowiedzi na skargi.

64. W odniesieniu do „komunikacji z właściwym organem nadzorczym" Rada zaleca, aby AT ON:

1. zmienił sekcję 6.4 zarządzenia w celu zapewnienia częstszej komunikacji z właściwym ON w ciągu roku; oraz

2. zajął się zgłaszaniem wszelkich istotnych zmian w wymogach akredytacji właściwego ON.

65. W odniesieniu do „statusu prawnego” Rada zaleca, aby AT ON:

1. wymagał, aby podmiot monitorujący miał jednostkę organizacyjną na terenie EOG;

2. wymagał, aby podmiot monitorujący miał dostęp do odpowiednich zasobów niezbędnych do wypełnienia swoich obowiązków monitorowania i wykazał, że jest w stanie dostarczyć mechanizm monitorowania kodeksu w odpowiednim czasie, zwłaszcza w odniesieniu do akredytacji osoby fizycznej jako podmiotu monitorującego; oraz

3. wyjaśnił, czy podmiot monitorujący może odwołać się do podwykonawców i na jakich zasadach oraz czy są one odzwierciedlone odpowiednio w notach wyjaśniających lub w zarządzeniu. Jeżeli zezwala

się na podwykonawstwo, należy zmienić zarządzenie, tak aby zobowiązania mające zastosowanie do podmiotu monitorującego miały takie samo zastosowanie do podwykonawców.

4 UWAGI KOŃCOWE

66. Niniejsza opinia jest skierowana do austriackiego organu nadzorczego i zostanie podana do wiadomości publicznej zgodnie z art. 64 ust. 5 lit. b) RODO.

67. Zgodnie z art. 64 ust. 7 i 8 RODO organ nadzorczy w terminie dwóch tygodni po otrzymaniu tej opinii informuje drogą elektroniczną Radę czy podtrzymuje projekt decyzji, czy też go zmieni. W powyższym terminie przedstawi zmieniony projekt decyzji lub, w przypadku gdy nie zamierza się zastosować do całości lub części opinii Rady, poda odpowiednie uzasadnienie, z powodu którego nie zamierza się zastosować do tej opinii. Organ nadzorczy informuje Radę o ostatecznej decyzji w celu włączenia do rejestru decyzji, która była przedmiotem mechanizmu spójności zgodnie z art. 70 ust. 1 lit. y) RODO.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

przyjęte