

# Opinia Rady (art. 64)



**Opinia 16/2020 w sprawie projektu decyzji właściwego organu nadzorczego Republiki Czeskiej w sprawie zatwierdzenia wymogów w zakresie akredytacji podmiotu certyfikującego zgodnie z art. 43 ust. 3 (RODO)**

**Przyjęta 25 maja 2020 r.**

Translations proofread by EDPB Members.  
This language version has not yet been proofread.

## Spis treści

1	STRESZCZENIE STANU FAKTYCZNEGO .....	4
2	OCENA .....	4
2.1	Ogólne uzasadnienie EROD w odniesieniu do przedłożonego projektu decyzji .....	4
2.2	Najważniejsze aspekty oceny (art. 43 ust. 2 RODO oraz załącznik 1 do wytycznych EROD), które zgodnie z wymogami w zakresie akredytacji przewidują spójną ocenę następujących elementów:.....	5
2.2.1	PREFIKS.....	6
2.2.2	UWAGI OGÓLNE.....	6
2.2.3	OGÓLNE WYMOGI AKREDYTACJI .....	7
2.2.4	WYMOGI DOTYCZĄCE ZASOBÓW .....	8
2.2.5	WYMOGI DOTYCZĄCE PROCEDUR .....	9
2.2.6	SYSTEM ZARZĄDZANIA.....	10
3	WNIOSKI/ZALECENIA.....	10
4	UWAGI KOŃCOWE .....	12

## Europejska Rada Ochrony Danych

uwzględniając art. 63, art. 64 ust. 1 lit. c), art. 64 ust. 3–8 oraz art. 43 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, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z 6 lipca 2018 r.<sup>1</sup>,

uwzględniając art. 10 i 22 swojego regulaminu wewnętrznego z 25 maja 2018 r.,

a także mając na uwadze, co następuje:

(1) Głównym zadaniem Rady jest zapewnienie spójnego stosowania rozporządzenia 2016/679 (zwanego dalej „RODO”) na całym terytorium Europejskiego Obszaru Gospodarczego. Zgodnie z art. 64 ust. 1 RODO Rada wydaje opinię w przypadku, gdy organ nadzorczy (ON) zamierza zatwierdzić wymogi w zakresie akredytacji podmiotów certyfikujących na podstawie art. 43. Celem niniejszej opinii jest zatem opracowanie zharmonizowanego podejścia w odniesieniu do wymagań, które organ nadzorczy odpowiedzialny za ochronę danych lub krajowa jednostka akredytująca zastosuje do akredytacji podmiotu certyfikującego. Chociaż RODO nie nakłada jednolitego zbioru wymogów w zakresie akredytacji, sprzyja ono spójności. Rada dąży do osiągnięcia tego celu w swoich opiniach, po pierwsze, zachęcając organy nadzorcze do sporządzenia własnych wymogów w zakresie akredytacji zgodnie ze strukturą określoną w załączniku do wytycznych EROD w sprawie akredytacji podmiotów certyfikujących, a po drugie, analizując je z wykorzystaniem wzoru dostarczonego przez EROD, który umożliwi dokonanie analizy porównawczej tych wymogów (w oparciu o normę ISO 17065 oraz wytyczne EROD w sprawie akredytacji podmiotów certyfikujących).

(2) Nawiązując do art. 43 RODO właściwe organy nadzorcze przyjmują wymogi w zakresie akredytacji. Powinny one jednak zastosować mechanizm spójności, aby wzbudzić zaufanie do mechanizmu certyfikacji, w szczególności poprzez ustanowienie wysokiego poziomu wymogów.

(3) Chociaż wymogi w zakresie akredytacji są objęte mechanizmem spójności, nie oznacza to, że powinny być one identyczne. Właściwe organy nadzorcze posiadają margines swobody w odniesieniu do kontekstu krajowego lub regionalnego i powinny uwzględnić przepisy lokalne. Celem opinii EROD nie jest wypracowanie jednolitego unijnego zbioru wymogów, lecz uniknięcie znaczących niespójności, które mogą mieć wpływ np. na zaufanie do niezależności lub wiedzy fachowej akredytowanych podmiotów certyfikujących.

(4) „Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących zgodnie z art. 43 ogólnego rozporządzenia o ochronie danych (2016/679)” (zwane dalej „wytycznymi”) oraz „Wytyczne 1/2018 w sprawie certyfikacji i określania kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia 2016/679” postępują jako wskazówki w kontekście mechanizmu spójności.

---

<sup>1</sup> Odniesienia do „Unii” w niniejszej opinii należy rozumieć jako odniesienia do „EOG”.

(5) Jeżeli państwo członkowskie zastrzega sobie, że podmioty certyfikujące mają być akredytowane przez organ nadzorczy, organ ten powinien ustanowić wymogi w zakresie akredytacji, w tym, między innymi, wymogi wyszczególnione w art. 43 ust. 2. W porównaniu ze zobowiązaniami związanymi z akredytacją podmiotów certyfikujących przez krajowe jednostki akredytujące w art. 43 przewidziano mniej szczegółowe wymogi w zakresie akredytacji, w przypadku gdy dokonuje jej sam organ nadzorczy. Aby przyczynić się do zharmonizowanego podejścia do akredytacji, wymogi w zakresie akredytacji stosowane przez organ nadzorczy należy oprzeć na normie ISO/IEC 17065 oraz uzupełnić je o dodatkowe wymogi, które organ nadzorczy ustanawia zgodnie z art. 43 ust. 1 lit. b). EROD zauważa, że art. 43 ust. 2 lit. a)–e) odzwierciedla i precyzuje wymogi normy ISO 17065, co przyczyni się do zachowania spójności<sup>2</sup>.

(6) Opinia Rady zostaje przyjęta zgodnie z art. 64 ust. 1 lit. c) i art. 64 ust. 3 i 8 RODO w związku z art. 10 ust. 2 regulaminu wewnętrznego EROD w terminie ośmiu tygodni od pierwszego dnia roboczego po podjęciu przez przewodniczącego i właściwy organ nadzorczy decyzji o kompletności dokumentacji. Ze względu na złożony charakter sprawy termin ten można przedłużyć o sześć tygodni na podstawie decyzji przewodniczącego.

## **PRZYJMUJE OPINIĘ:**

### 1 STRESZCZENIE STANU FAKTYCZNEGO

1. Organ nadzorczy Republiki Czeskiej (dalej zwany „CZ ON”) przedłożył EROD swój projekt wymogów w zakresie akredytacji zgodnie z art. 43 ust. 1 lit. b). Dokumentacja została uznana za kompletną w dniu 17 lutego 2020 r. Krajowa jednostka akredytująca (NAB) Republiki Czeskiej dokona akredytacji podmiotów certyfikujących, stosując kryteria certyfikacji RODO. Oznacza to, że NAB zastosuje normę ISO 17065 oraz dodatkowe wymogi ustanowione przez CZ ON, po ich zatwierdzeniu przez ten organ, po uzyskaniu opinii Rady w sprawie projektu wymogów akredytacji, aby akredytować podmioty certyfikujące.
2. Zgodnie z art. 10 ust. 2 regulaminu wewnętrznego Rady, ze względu na złożoność rozpatrywanej sprawy, przewodnicząca zdecydowała o przedłużeniu początkowego ośmioletniego terminu o kolejne sześć tygodni.

### 2 OCENA

#### 2.1 Ogólne uzasadnienie EROD w odniesieniu do przedłożonego projektu decyzji

3. Celem niniejszej opinii jest dokonanie oceny wymogów w zakresie akredytacji, opracowanych przez ON w związku z normą ISO 17065 lub w formie kompletnego zbioru wymogów, aby umożliwić krajowej jednostce akredytującej lub ON, zgodnie z art. 43 ust. 1 RODO, akredytację podmiotu certyfikującego odpowiedzialnego za wydawanie i odnawianie certyfikacji zgodnie z art. 42 RODO. Pozostaje to bez

---

<sup>2</sup> Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679), pkt 39. Dostępne tutaj: [https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies\\_pl](https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_pl)

uszczerbku dla zadań i uprawnień właściwego ON. W tym konkretnym przypadku Rada zauważa, że CZ ON postanowił zwrócić się do swojej krajowej jednostki akredytującej o wydanie akredytacji, po uwzględnieniu dodatkowych wymogów zgodnie z wytycznymi, które powinny zostać wykorzystane przez krajową jednostkę akredytującą przy wydawaniu akredytacji.

4. Ocena dodatkowych wymogów w zakresie akredytacji CZ ON ma na celu zbadanie zmian (elementów dodanych lub usuniętych) w odniesieniu do wytycznych, a w szczególności załącznika 1 do wytycznych. Ponadto w opinii EROD skupiono się na wszelkich kwestiach, które mogą mieć wpływ na zachowanie spójnego podejścia w zakresie akredytacji podmiotów certyfikujących.
5. Należy zauważyć, iż celem wytycznych w sprawie akredytacji podmiotów certyfikujących jest zapewnienie ON wsparcia przy określaniu ich wymogów w zakresie akredytacji. Załącznik do wytycznych nie stanowi wymogów w zakresie akredytacji jako takich. Wymogi w zakresie akredytacji podmiotów certyfikujących muszą zostać określone przez ON w sposób umożliwiający ich praktyczne i spójne stosowanie, zgodnie z wymaganiami ON.
6. Rada potwierdza fakt, że ze względu na wiedzę fachową krajowych jednostek akredytujących powinny one mieć swobodę działania przy określaniu niektórych przepisów szczególnych w ramach obowiązujących wymogów w zakresie akredytacji. Rada uznaje jednak za konieczne, by podkreślić, że w przypadku ustanowienia jakichkolwiek dodatkowych wymogów, powinny one zostać określone w sposób umożliwiający ich praktyczne, spójne stosowanie oraz – w razie potrzeby – przegląd.
7. EROD zauważa, że normy ISO, zwłaszcza ISO 17065, podlegają prawom własności intelektualnej, w związku z czym w niniejszej opinii nie będzie odnosić się do ich treści. EROD postanowiła zatem, w stosownych przypadkach, odnieść się do konkretnych sekcji normy ISO, jednakże bez przywoływania jej tekstu.
8. Ponadto Rada dokonała oceny zgodnie ze strukturą przewidzianą w załączniku 1 do wytycznych (zwanym dalej „załącznikiem”). Jeżeli w niniejszej opinii nie odniesiono się do konkretnej sekcji projektu wymogów w zakresie akredytacji CZ ON, należy rozumieć, że Rada nie ma uwag oraz nie wymaga od CZ ON podjęcia dalszych działań.
9. Niniejsza opinia nie dotyczy informacji przedłożonych przez CZ ON, które są poza zakresem stosowania art. 43 ust. 2 RODO, takich jak odniesienia do przepisów krajowych. Rada zauważa jednak, że przepisy krajowe powinny być zgodne z RODO, jeżeli jest to wymagane.

## 2.2 Najważniejsze aspekty oceny (art. 43 ust. 2 RODO oraz załącznik 1 do wytycznych EROD), które zgodnie z wymogami w zakresie akredytacji przewidują spójną ocenę następujących elementów:

- a. odniesienie się do wszystkich kluczowych obszarów wskazanych w załączniku do wytycznych, oraz uwzględnienie wszelkich odstępstw od załącznika;
- b. niezależność podmiotu certyfikującego;
- c. konflikty interesów podmiotu certyfikującego;
- d. wiedza fachowa podmiotu certyfikującego;
- e. odpowiednie zabezpieczenia zapewniające właściwe stosowanie kryteriów certyfikacji RODO przez podmiot certyfikujący;

- f. procedury dotyczące dokonywania, okresowego przeglądu oraz wycofania certyfikacji RODO; oraz
- g. przejrzyste rozpatrywanie skarg dotyczących naruszeń certyfikacji.

10. Biorąc pod uwagę, że:

- a. artykuł 43 ust. 2 RODO zawiera wykaz obszarów akredytacji, które podmiot certyfikujący musi uwzględnić, aby uzyskać akredytację;
- b. artykuł 43 ust. 3 RODO stanowi, że wymogi w zakresie akredytacji podmiotów certyfikujących są zatwierdzane przez właściwy organ nadzorczy;
- c. artykuł 57 ust. 1 lit. p) i q) RODO stanowią, że właściwy organ nadzorczy opracowuje i publikuje wymogi w zakresie akredytacji podmiotów certyfikujących oraz może postanowić o samodzielnym dokonaniu akredytacji podmiotów certyfikujących;
- d. artykuł 64 ust. 1 lit. c) RODO stanowi, że EROD wydaje opinię w przypadku, gdy organ nadzorczy zamierza zatwierdzić wymogi w zakresie akredytacji podmiotu certyfikującego zgodnie z art. 43 ust. 3;
- e. jeżeli akredytacji dokonuje krajowa jednostka akredytująca zgodnie z normą ISO/IEC 17065/2012, należy również zastosować dodatkowe wymagania określone przez właściwy organ nadzorczy;
- f. w załączniku 1 do wytycznych w sprawie akredytacji certyfikacji przewidziano proponowane wymogi, które organ nadzorczy ds. ochrony danych opracowuje i stosuje podczas akredytacji podmiotu certyfikującego przez krajową jednostkę akredytującą;

EROD jest zdania, że:

#### 2.2.1 PREFIKS

11. Rada przyznaje, że warunki współpracy, regulujące stosunki między krajową jednostką akredytującą a jej organem nadzorczym ds. ochrony danych, nie są wymogiem w zakresie akredytacji podmiotów certyfikujących *per se*. Jednak w celu zachowania kompletności i przejrzystości Rada uważa, że takie warunki współpracy, o ile istnieją, podaje się do wiadomości publicznej w formacie, jaki ON uzna za odpowiedni.

#### 2.2.2 UWAGI OGÓLNE

12. Rada zauważa, że projekt wymogów w zakresie akredytacji nie jest w pełni zgodny ze strukturą przewidzianą w załączniku nr 1 do wytycznych. Na przykład brak jest sekcji dotyczących „zakresu stosowania” oraz „terminów i definicji”. W związku z tym, w celu zapewnienia jasności i umożliwienia łatwiejszej oceny wymogów, Rada uważa, że numeracja i ogólna struktura dokumentu mogłyby zostać ulepszone. Aby ułatwić dokonanie oceny, Rada zachęca zatem CZ ON do stosowania struktury załącznika zawartej w projekcie wymogów w zakresie akredytacji i dodania brakujących sekcji, co ma szczególne znaczenie dla definicji terminów stosowanych w całym dokumencie. Ponadto Rada zauważa, że projekt wymogów w zakresie akredytacji CZ ON kilkakrotnie odnosi się do odpowiedniej

sekcji normy ISO 17065 lub do odpowiednich sekcji załącznika, nie doprecyzowując jednak takiego odniesienia. Rada zachęca zatem CZ ON do doprecyzowania odniesień do sekcji normy ISO 17065 i załącznika.

13. Rada zauważa, że projekt wymogów w zakresie akredytacji CZ ON kilkakrotnie odnosi się do „przedmiotu oceny” (np. sekcje 3.2.1.2.1.2.10; 3.2.1.2.6.3.1; 3.2.1.2.8.1.6.3; 3.2.1.2.10.4.1; 3.1.2.10.7.3.1; 3.1.2.10.7.3.2 i 3.2.1.2.10.10.2). Rada rozumie, że termin ten jest używany jako synonim „celu oceny”. Aby jednak zapewnić jasność, Rada zachęca CZ ON do konsekwentnego stosowania terminu „cel oceny”.
14. Rada zauważa, że kilka wymogów nie zostało sformułowanych jako obowiązek podmiotu certyfikującego (np. 3.2.1.2.2 i 3.2.1.2.3). Rada zachęca CZ ON do przereformowania wymogów w celu wyjaśnienia, że są one obowiązkowe – tj. rozpoczęcia tekstu wymogu od słów „podmiot certyfikujący zobowiązany jest do [...]”.

### 2.2.3 OGÓLNE WYMOGI AKREDYTACJI

15. W odniesieniu do umowy o certyfikacji (sekcja 3.2.1.2.1.2 projektu wymogów akredytacji CZ ON) Rada zauważa, że podsekcja 3.2.1.2.1.2.2 nie zawiera żadnego odniesienia do „kwestii objętych postanowieniami umownymi o poufności”, do których ON również musi mieć dostęp. W związku z tym Rada zaleca CZ ON zmianę projektu poprzez włączenie obowiązku zapewnienia ON dostępu również do kwestii objętych postanowieniami umownymi o poufności.
16. W odniesieniu do podsekcji 3.2.1.2.1.2.8 projektu wymogów w zakresie akredytacji CZ ON Rada zauważa, że nie jest jasne, komu te informacje mają zostać ujawnione. Rada zachęca zatem CZ ON do wyjaśnienia, kto będzie odbiorcą tych informacji. Ponadto wspomniane informacje są „niezbędne do przyznania certyfikacji”, jak określono w pkt 7 sekcji 4.1.2 załącznika. Rada zaleca CZ ON zastąpienie sformułowania „informacje o przyznawaniu certyfikacji” wyrażeniem „informacje niezbędne do przyznania certyfikacji”.
17. W odniesieniu do podsekcji 3.2.1.2.1.2.9 projektu wymogów w zakresie akredytacji CZ ON, nie jest jasne, jakiego rodzaju informacje powinny zostać bezpośrednio przekazane Radzie. W art. 42 ust. 8 RODO nakłada się na Radę obowiązek zestawienia m.in. wszystkich mechanizmów certyfikacji. W tym kontekście zakłada się, że właściwe ON prześlą odpowiednie informacje Radzie, która następnie opublikuje je w rejestrze publicznym. W związku z tym Rada zaleca, aby CZ ON doprecyzował podsekcję 3.2.1.2.1.2.9 projektu wymogów zgodnie z art. 42 ust. 8 RODO.
18. Jeżeli chodzi o podsekcję 3.2.1.2.1.2.12 projektu wymogów w zakresie akredytacji CZ ON, Rada przyjmuje do wiadomości fakt, że CZ ON opracował zredagowaną wersję części wymogu przewidzianego w załączniku. CZ ON pominął jednak następujący fragment (w stosownych przypadkach) „należy odnieść się również do konsekwencji ponoszonych przez klienta”. W związku z tym Rada zaleca, aby CZ ON dodał wspomniany powyżej brakujący fragment wymogu.
19. Ponadto w podsekcji 3.2.1.2.1.2.13 projektu wymogów akredytacji CZ ON ustanowiono obowiązek „zawarcia zobowiązania wnioskodawcy do informowania podmiotu certyfikującego o wszelkich zmianach, które mogą mieć wpływ na zgodność certyfikowanego przedmiotu z kryteriami certyfikacji”. Rada uważa to sformułowanie za zbyt ogólne i zaleca, aby CZ ON zmienił projekt wymogów w celu uwzględnienia „wszelkich zmian swojej sytuacji faktycznej lub prawnej oraz zmian produktów, procesów i usług objętych certyfikacją”.



20. Jeżeli chodzi o stosowanie znaków jakości i oznaczeń w dziedzinie ochrony danych (sekcja 3.2.1.2.1.3 projektu wymogów akredytacji CZ ON), Rada zauważa, że projekt wymogów CZ ON stanowi, że umowa o certyfikacji zawiera „przepisy dotyczące stosowania certyfikatów, znaków i oznaczeń, jeżeli są one zapewniane przez właściciela systemu certyfikacji”. To samo sformułowanie znajduje się w podsekcji 3.2.1.2.1.2.14. Rada uważa, że to zobowiązanie zostało już ujęte w pkt 4.1.2.2 lit. l) normy ISO 17065, a zatem nie powinno być zawarte w żadnym systemie certyfikacji (zob. również pkt 4.1.3 normy ISO 17065). W związku z tym, w celu zapewnienia jasności, Rada zaleca, aby CZ ON usunął wyżej wymienione sekcje.
21. W odniesieniu do wymogów dotyczących zarządzania bezstronnością, zgodnie z informacjami przedstawionymi przez CZ ON we wzorze, pkt 4.2.1.b) i 4.2.2 załącznika są w wystarczającym stopniu uwzględnione w pkt 4.2 normy ISO 17065. Rada uważa jednak, że wymogi te należy wyraźnie uwzględnić w projekcie wymogów w zakresie akredytacji opracowanym przez ON zgodnie z załącznikiem. Rada zaleca zatem, aby CZ ON uwzględnił brakujące wymogi dotyczące zarządzania bezstronnością przewidziane w załączniku.
22. W odniesieniu do wymogu dotyczącego odpowiedzialności i finansowania (sekcja 3.2.1.2.3.1 projektu wymogów CZ ON) Rada zachęca CZ ON do doprecyzowania, że wymóg ten należy stosować regularnie.

#### 2.2.4 WYMOGI DOTYCZĄCE ZASOBÓW

23. Jeżeli chodzi o personel podmiotu certyfikującego (sekcja 3.2.1.2.8.1.6 projektu wymogów akredytacji CZ ON), Rada zauważa, że wymogi dotyczące personelu odpowiedzialnego za oceny (podsekcja 3.2.1.2.8.1.6.3) obejmują „5-letnią praktykę i co najmniej 10 audytów przeprowadzonych w ramach działalności certyfikacyjnej w tej samej lub podobnej dziedzinie [...] lub 5-letnią praktykę w zakresie certyfikacji przedmiotów działalności podmiotu certyfikującego”. Wymogi dotyczące personelu odpowiedzialnego za podejmowanie decyzji (podsekcja 3.2.1.2.8.1.6.4) również obejmują „co najmniej 5-letnią praktykę i co najmniej 10 audytów przeprowadzonych w ramach działalności certyfikacyjnej w tej samej lub podobnej dziedzinie”. Rada uważa, że wymogi dotyczące wiedzy fachowej dla podmiotów oceniających i decydentów powinny być dostosowane do różnych zadań, które wykonują. W związku z powyższym zdaniem Rady podmioty oceniające powinny posiadać bardziej specjalistyczną wiedzę i doświadczenie zawodowe w zakresie procedur technicznych (np. audytów i certyfikacji), natomiast decydenci powinni posiadać bardziej ogólną i kompleksową wiedzę fachową oraz doświadczenie zawodowe w zakresie ochrony danych. Mając to na uwadze Rada zachęca CZ ON do preredagowania tej podsekcji i uwzględnienia różnych wymogów dotyczących wiedzy merytorycznej lub doświadczenia dla podmiotów oceniających i decydentów.
24. Ponadto Rada przyjmuje do wiadomości, że w pkt 3.2.1.2.9.1 projektu wymogów w zakresie akredytacji CZ ON stwierdzono, że outsourcing nie jest dozwolony w odniesieniu do działalności certyfikacyjnej. W następnym punkcie zezwala się jednak na korzystanie z usług audytorów zewnętrznych i ekspertów zewnętrznych do celów oceny, chyba że stanowi to działalność certyfikacyjną. Rada uważa, że projekt wymogów w zakresie akredytacji powinien określać, kiedy „dane działanie stanowi działalność certyfikacyjną”, lub wyjaśniać, że podmiot certyfikujący pozostanie odpowiedzialny za podejmowanie decyzji, nawet jeżeli korzysta z usług ekspertów zewnętrznych. W związku z tym Rada zaleca, aby CZ ON zmienił odpowiednio projekt.



## 2.2.5 WYMOGI DOTYCZĄCE PROCEDUR

25. Rada zauważa, że sekcja 3.2.1.2.10.1.1 projektu dodatkowych wymogów CZ ON odnosi się do „wszystkich dodatkowych wymogów dotyczących konfliktu interesów (7.1 pkt 1)”. Projekt dodatkowych wymogów CZ ON nie zawiera jednak dodatkowych wymogów dotyczących konfliktu interesów. W związku z tym Rada zachęca CZ ON do zmiany projektu w celu uniknięcia nieporozumień.
26. W odniesieniu do wymogów dotyczących składania wniosków Rada zauważa, że podsekcja 3.2.1.2.10.2.3 projektu wymogów akredytacji CZ ON wydaje się sugerować, że informacje na temat przekazanych danych podaje się we wniosku tylko wtedy, gdy dane przekazywane są do państwa trzeciego lub organizacji międzynarodowej. Rada podkreśla jednak, że wnioskodawca zawsze musi zawierać opis danych przekazywanych do innych systemów lub organizacji, niezależnie od ich lokalizacji. W związku z tym Rada zachęca CZ ON do zmiany brzmienia wymogu w celu uniknięcia nieporozumień.
27. Rada zauważa, że obowiązek określenia w umowie o certyfikacji wiążących metod oceny (sekcja 3.2.1.2.1.2.6 projektu wymogów akredytacji CZ ON) nie zawiera odniesienia do celu oceny, zgodnie z pkt 1 sekcji 7.3 załącznika do wytycznych. W celu zapewnienia jasności Rada zachęca CZ ON do uwzględnienia takiego odniesienia.
28. Ponadto Rada zauważa, że projekt wymogów akredytacji CZ ON przewiduje sytuację, w której podmioty przetwarzające są wykorzystywane do prowadzenia procesów przetwarzania danych, zgodnie z załącznikiem do wytycznych (sekcja 3.2.1.2.10.2 projektu wymogów akredytacji CZ ON). Ponadto Rada zachęca CZ ON do rozważenia, czy w tym przypadku należy również wspomnieć o współadministratorach i ich szczególnych ustaleniach.
29. W odniesieniu do wymogów w zakresie oceny (sekcja 3.2.1.2.10.4 projektu wymogów CZ ON) Rada zauważa, że wymogi akredytacji CZ ON nie nakładają na podmiot certyfikujący obowiązku szczegółowego określenia w swoim mechanizmie certyfikacji, w jaki sposób informacje na temat niezgodności z mechanizmem certyfikacji wymagane w pkt 7.4.6 normy ISO 17065 należy przekazywać wnioskodawcy. Jak wskazano w załączniku (podsekcja 7.4), określa się co najmniej charakter i termin przekazania takich informacji. W związku z tym Rada zaleca, aby CZ ON dodał wyżej wymieniony obowiązek.
30. Ponadto wydaje się, że podsekcja 3.2.1.2.10.4.2 projektu wymogów CZ ON ogranicza metody oceny do badań, audytów lub inspekcji. Rada uważa, że można również zastosować inne metody oceny i w związku z tym zachęca CZ ON do zmiany projektu w celu doprecyzowania, że wykaz nie ma charakteru wyczerpującego.
31. Jeżeli chodzi o podsekcję 3.2.1.2.10.4.4.1.4 projektu wymogów w zakresie akredytacji CZ ON, Rada uważa, że wymogi te powinny jasno stanowić, że podmiot certyfikujący jest zobowiązany do sprawdzenia zgodności z kryteriami i zachęca CZ ON do odpowiedniej zmiany projektu.
32. W odniesieniu do wymogów dotyczących przeglądu (podsekcja 3.2.1.2.10.5 projektu wymogów akredytacji CZ ON) Rada zauważa, że projekt wymogów akredytacji CZ ON nie odnosi się do obowiązku określenia procedur udzielania i cofania certyfikatów. Rada zaleca, aby CZ ON zmienił odpowiednio projekt.
33. Jeżeli chodzi o wymogi dotyczące dokumentacji certyfikacji, Rada zauważa, że w sekcji 3.1.2.10.7.2 projektu wymogów akredytacji CZ ON stwierdzono, że podmiot certyfikujący powinien doprecyzować, że monitorowanie stanowi warunek ważności certyfikacji „jeżeli monitorowanie wymagane jest w

ramach systemu certyfikacji [...]”. Rada uważa, że w przypadku certyfikacji na mocy RODO działania w zakresie monitorowania zawsze są obowiązkowe, w związku z czym zaleca, aby CZ ON uwzględnił taki obowiązek.

34. W odniesieniu do wymogów związanych z wykazem certyfikowanych produktów (sekcja 3.2.1.2.10.8 projektu wymogów w zakresie akredytacji CZ ON i sekcja 7.8 załącznika), w szczególności obowiązku informowania właściwego ON o przyczynach udzielenia lub cofnięcia wnioskowanej certyfikacji, Rada zauważa, że projekt wymogów akredytacji CZ ON odnosi się do sekcji 3.2.1.2.10.4.5. Sekcja ta dotyczy jednak obowiązku udostępnienia CZ ON dokumentacji oceny na wniosek, natomiast wymóg zawarty w sekcji 7.8 załącznika do wytycznych zawiera obowiązek proaktywnego informowania ON o przyczynach udzielenia lub cofnięcia certyfikacji. W związku z tym Rada zaleca, aby CZ ON zmienił odpowiednio projekt.
35. Jeżeli chodzi o zmiany mające wpływ na certyfikację, Rada zauważa, że w projekcie wymogów w zakresie akredytacji CZ ON nie wymienia się wśród procedur, które mają zostać uzgodnione, procesu zatwierdzania z właściwym ON, o którym mowa w załączniku do wytycznych (s. 19). Rada uznaje, że wykaz przedstawiony w sekcji 7.10 załącznika nie jest obowiązkowy. Aby jednak zapewnić spójność, Rada zachęca CZ ON do dodania odniesienia do procesu zatwierdzania z ON.
36. Rada zauważa, że projekt wymogów w zakresie akredytacji CZ ON nie obejmuje wyraźnie obowiązku przyjęcia przez podmiot certyfikujący decyzji i nakazów CZ ON w sprawie cofnięcia lub odmowy dokonania certyfikacji wnioskodawcy, jeżeli wymogi dotyczące certyfikacji nie są już spełniane. Rada zaleca, aby CZ ON wyraźnie uwzględnił ten obowiązek w projekcie wymogów w zakresie akredytacji. W odniesieniu do zakończenia, ograniczenia, zawieszenia lub wycofania certyfikacji Rada zauważa, że sekcje 3.2.1.2.10.10.2 i 3.2.1.2.10.10.3 projektu wymogów odnoszą się do „nakazywania”. Jeżeli zamiarem jest odnoszenie się do „decyzji i nakazów” ON, jak określono w art. 58 ust. 2 lit. h) RODO, Rada zachęca CZ ON do stosowania tej samej terminologii, jaką zastosowano w RODO oraz odnoszenia się do „decyzji i nakazów”.

### 2.2.6 SYSTEM ZARZĄDZANIA

37. Rada uważa, że sekcja 3.2.1.2.11 projektu dodatkowych wymogów CZ ON nie nakłada na podmiot certyfikujący obowiązku „stałego podawania do wiadomości publicznej, które certyfikacje zostały przeprowadzone na jakiej podstawie oraz jaki jest okres ważności certyfikacji na podstawie jakich ram i warunków”, jak określono w sekcji 8 załącznika. W związku z tym Rada zaleca, aby CZ ON zmienił projekt wymogów, uwzględniając w nim wyżej wymienione odniesienie.

## 3 WNIOSKI/ZALECENIA

38. Projekt wymogów akredytacji organu nadzorczego Republiki Czeskiej może prowadzić do niespójnego stosowania akredytacji podmiotów certyfikujących i konieczne jest wprowadzenie następujących zmian:
39. W odniesieniu do „ogólnych wymogów w zakresie akredytacji” Rada zaleca, aby CZ ON:
  - 1) uwzględnił obowiązek zapewnienia ON dostępu do „kwestii objętych postanowieniami umownymi o poufności” w sekcji 3.2.1.2.1.2;

- 2) zastąpił sformułowanie „informacje o przyznawaniu certyfikacji” wyrażeniem „informacje niezbędne do przyznania certyfikacji” w podsekcji 3.2.1.2.1.2.8;
- 3) doprecyzował podsekcję 3.2.1.2.1.2.9 zgodnie z art. 42 ust. 8 RODO;
- 4) w podsekcji 3.2.1.2.1.2.12 dodał następujący fragment [w stosownych przypadkach] „należy odnieść się również do konsekwencji ponoszonych przez klienta”;
- 5) zmienił podsekcję 3.2.1.2.1.2.13 i uwzględnił „wszelkie zmiany swojej sytuacji faktycznej lub prawnej oraz zmiany produktów, procesów i usług objętych certyfikacją”;
- 6) usunął sekcję 3.2.1.2.1.3 i podsekcję 3.2.1.2.1.2.14;
- 7) uwzględnił brakujące wymogi dotyczące zarządzania bezstronnością przewidziane w załączniku.

40. W odniesieniu do „wymogów dotyczących zasobów” Rada zaleca, aby CZ ON:

- 1) zmienił sekcję 3.2.1.2.9.1 i określił, kiedy „dane działanie stanowi działalność certyfikacyjną” lub wyjaśnił, że podmiot certyfikujący pozostanie odpowiedzialny za podejmowanie decyzji, nawet jeżeli korzysta z usług ekspertów zewnętrznych.

41. W odniesieniu do „wymogów dotyczących procedur” Rada zaleca, aby CZ ON:

- 1) uwzględnił w sekcji 3.2.1.2.10.4 obowiązek szczegółowego określenia w swoim mechanizmie certyfikacji, w jaki sposób informacje na temat niezgodności z mechanizmem certyfikacji wymagane w pkt 7.4.6 normy ISO 17065 należy przekazywać wnioskodawcy;
- 2) zmienił sekcję 3.2.1.2.10.5 w celu odniesienia się do obowiązku określenia procedur udzielania i cofania certyfikacji;
- 3) zmienił sekcję 3.1.2.10.7.2 w celu uwzględnienia faktu, że w przypadku certyfikacji na mocy RODO działania w zakresie monitorowania są zawsze obowiązkowe;
- 4) zmienił sekcję 3.2.1.2.10.8 w celu uwzględnienia obowiązku podmiotu certyfikującego dotyczącego proaktywnego informowania ON o przyczynach udzielenia lub cofnięcia certyfikacji;
- 5) uwzględnił obowiązek przyjęcia przez podmiot certyfikujący decyzji i nakazów CZ ON w sprawie cofnięcia lub odmowy wydania certyfikacji wnioskodawcy, jeżeli wymogi dotyczące certyfikacji nie są już spełniane.

42. W odniesieniu do „systemu zarządzania” Rada zaleca, aby CZ ON:

- 1) uwzględnił obowiązek podmiotu certyfikującego dotyczący „stałego podawania do wiadomości publicznej, które certyfikacje zostały przeprowadzone na jakiej podstawie oraz jaki jest okres ważności certyfikacji na podstawie jakich ram i warunków”, jak określono w sekcji 8 załącznika.

## 4 UWAGI KOŃCOWE

43. Niniejsza opinia jest skierowana do organu nadzorczego Republiki Czeskiej i zostanie podana do wiadomości publicznej zgodnie z art. 64 ust. 5 lit. b) RODO.
44. Zgodnie z art. 64 ust. 7 i 8 RODO CZ ON w terminie dwóch tygodni po otrzymaniu niniejszej opinii informuje drogą elektroniczną przewodniczącą, czy podtrzymuje projekt wykazu, czy też go zmienia. W powyższym terminie przedstawi zmieniony projekt wykazu lub, w przypadku gdy nie zamierza się zastosować do opinii Rady, poda odpowiednie uzasadnienie niezastosowania się do całości lub części niniejszej opinii.
45. CZ ON poinformuje Radę o ostatecznej decyzji w celu włączenia do rejestru decyzji będącego przedmiotem mechanizmu spójności, zgodnie z art. 70 ust. 1 lit. y) RODO.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)