Program certyfikacji Inspektorów Ochrony Danych (IOD)

Historia zmian:	**w dniu:**	**przez:**
Aktualizacja stopki	10.09.2019	PU
Zmiana cennika	03.01.2019	PU
Zamknięcie NZ + uwzględnienie SPP po ocenie PCA	04.10.2019	PU
Usunięcie z Programu punktu związanego z opłatami (punkt 8) + aktualizacja zapisów w punkcie 11	06.12.2019	PU

DEKRA Certification Sp. z o.o., ul. Legnicka 48H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

1. Wstęp

Program certyfikacji osób, zgodnie z procedurą nr V-09SS-x03pl Przebieg procesu certyfikacji osób obejmuje Inspektora Ochrony Danych (IOD).

ROZPORZĄDZENIE 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 (ogólne rozporządzenie o ochronie danych) nałożyło na podmioty przetwarzające dane osobowe obowiązek powołania inspektora ochrony danych osobowych. Obowiązek dotyczy organów i podmiotów publicznych oraz wszystkich innych podmiotów, które przetwarzają dane osobowe na dużą skalę. Ponieważ rozporządzenie nie precyzuje zasad określania skali przetwarzania, dla **większości** podmiotów wskazane będzie powołanie dedykowanej osoby do monitorowania prawidłowości przetwarzania danych w organizacji.

W 2017 roku w Polsce było ponad 25 tysięcy zarejestrowanych w bazie GIODO ABI[1], przy czym samych organów administracji publicznej, gdzie powołanie Inspektora będzie obowiązkowe, jest ponad 68 tysięcy. Dalej, jeśli wziąć pod uwagę choćby wskazaną w RODO grupę podmiotów, w których „główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub wymaga regularnego i systematycznego monitorowania osób", takich jak szpitale i przychodnie, banki i ubezpieczyciele, podmioty świadczące usługi ochrony mienia, prowadzące monitoring, podmioty działające w obszarze telekomunikacji lub reklamy, badań rynku i opinii publicznej - liczba podmiotów, których dotyczyć będzie powołanie Inspektora sięga kilkuset tysięcy (źródło Tablice dotyczące podmiotów gospodarki narodowej (bez osób fizycznych prowadzących wyłącznie indywidualne gospodarstwa rolne) - wg stanu na 30.11.2017 r.).[2]

Istotą prawidłowego wykonywania funkcji przez Inspektora jest jego wysoka pozycja w organizacji i niezależność. Powołany Inspektor, zgodnie z przepisami rozporządzenia, powinien podlegać pod najwyższe kierownictwo ale też nie powinien mieć zlecanych innych zadań, powodujących konflikt interesów. Innymi słowy, optymalnym rozwiązaniem jest pełnienie przez daną osobę wyłącznie roli Inspektora, gdyż angażowanie jej w jakikolwiek inny obszar działalności podmiotu może rodzić sytuację, w której Inspektor monitorowałby procesy w których sam uczestniczy.

Dla większości organizacji, ze względu na wymóg niezależności i wymaganą pracochłonność, oznacza to zaangażowanie do roli Inspektora osoby zewnętrznej

[1] źródło Gazeta Prawna 28.07.2017r., Zofia Jóźwiak, Inspektor ochrony danych obowiązkowo w każdej publicznej instytucji

[2] Przykłady działań, które mogą stanowić regularne i systematyczne monitorowanie osób, których dane dotyczą: obsługa sieci telekomunikacyjnej; świadczenie usług telekomunikacyjnych; przekierowywanie poczty elektronicznej; działania marketingowe oparte na danych; profilowanie i ocenianie dla celów oceny ryzyka (na przykład dla celów oceny ryzyka kredytowego, ustanawiania składek ubezpieczeniowych, zapobiegania oszustwom, wykrywania prania pieniędzy); śledzenie lokalizacji, na przykład przez aplikacje mobilne; programy lojalnościowe; reklama behawioralna; monitorowanie danych dotyczących zdrowia i kondycji fizycznej za pośrednictwem urządzeń przenośnych; monitoring wizyjny; urządzenia skomunikowane np. inteligentne liczniki, inteligentne samochody, automatyka domowa, etc. (Źródło: Wytyczne dotyczące inspektorów ochrony danych ('DPO') Przyjęte w dniu 13 grudnia 2016 r. Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.)

DEKRA Certification Sp. z o.o., ul. Legnicka 48H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

(w wymiarze odpowiadającym pełnemu lub części etatu – w zależności od skali problemu), eksperta w dziedzinie ochrony danych osobowych, który zapewni nadzór nad prawidłowym wdrożeniem i przestrzeganiem wymagań w zakresie ochrony danych. Duże podmioty na rynku polskim już szukają ekspertów do kierowania procesem przystosowania przedsiębiorstwa do RODO (Źródło: prawo.gazetaprawna.pl, *Strażnik danych osobowych pilnie poszukiwany*, Sylwia Czubkowska, 28.08.2017). Niezależnie od innych uwarunkowań, można oczekiwać, że outsourcing usług w tym zakresie będzie zjawiskiem znaczącym wśród stosowanych rozwiązań.

Odbiorcą usług w zakresie IOD będą przede wszystkim małe i średnie przedsiębiorstwa, które wg Raportu o stanie sektora MSP w Polsce , (Źródło: Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2016) posiadają znaczne bariery organizacyjne i finansowe uniemożliwiające skuteczne realizowanie obowiązku wynikającego z RODO w ramach własnych zasobów. Liczba MSP stanowi ponad 90% ogółu przedsiębiorstw w Polsce.

Rosnące zapotrzebowanie na usługi Inspektora powoduje, że liczba podmiotów oferujących usługi Inspektora rośnie.

Jednocześnie regulacje prawne w przedmiotowym zakresie nie precyzują listy wymagań w obszarze doświadczenia, kompetencji i kwalifikacji inspektorów.

Należy zauważyć, że sytuacja, w której postawiono organizacjom określone wymogi, a nie funkcjonują jasne, jednoznaczne, obiektywne kryteria w zakresie kompetencji osób potencjalnie mogących pełnić funkcję IOD, otwiera pole do pojawienia się na rynku działań dalekich od profesjonalizmu. Odpowiedni zapis (art. 37(5)) mówi jedynie, że *inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa …….",* nie zawiera konkretnych, jednoznacznych kryteriów.

Sytuacja ta powoduje występowanie dużych zagrożeń dla organizacji wdrażających postanowienia RODO, ponieważ z punktu widzenia podmiotów poszukujących usług zewnętrznego eksperta brak jednoznacznych kryteriów w zakresie kwalifikacji Inspektora rodzi ryzyko zaangażowania do tej roli osoby niedoświadczonej i niekompetentnej. Osoby takie często mogą posługiwać się różnymi dokumentami kwalifikacji, których obiektywność i jakość jest niemożliwa do zweryfikowania. To z kolei stawia pod znakiem zapytania prawidłowość wdrożenia i przestrzegania zapisów RODO i przepisów polskich w przedmiotowym zakresie. Nieprzestrzeganie przepisów RODO to nie tylko ryzyko utraty, czy innych nieprawidłowości w obszarze przetwarzania danych, ale też wysokie prawdopodobieństwo nałożenia na podmiot wysokich kar pieniężnych mogących sięgać do 4% rocznego obrotu przedsiębiorstwa. Całość problemu może stanowić poważne zagrożenie dla gospodarki krajowej. Jakkolwiek można zakładać, że w umowie zawartej przez organizację z podmiotem angażowanym do funkcji IOD znajdą się zapisy definiujące odpowiedzialność materialną IOD w sytuacji, gdy na skutek działań IOD GIODO nakłada na organizację karę finansową, to zapisy takie mogą być nieskuteczne jeżeli zestawi się możliwą wysokość kary z możliwościami egzekucyjnymi (najczęściej IOD będzie osobą fizyczną prowadzącą działalność gospodarczą, lub przedstawicielem podmiotu o niewielkim potencjale finansowym).

Istnieje zatem pilna potrzeba usystematyzowania wymagań w przedmiotowym zakresie, które zatwierdzone przez Polskie Centrum Akredytacji, stanowiłyby wiarygodny miernik kompetencji Inspektora.

Dotychczas jedynym narzędziem zapewnienia podnoszenia kwalifikacji i bieżącej aktualizacji wiedzy i umiejętności osób odpowiedzialnych za bezpieczeństwo przetwarzania danych osobowych w organizacji były szkolenia. W obliczu zmian wprowadzonych przez RODO, firmy szkoleniowe zaczęły oferować szkolenia dla Inspektorów, niemniej jednak szkolenia te różnią się znacznie intensywnością, czy zakresem.

Warto przywołać jeszcze dokument wydany przez GIODO – „Czy jesteś gotowy na RODO?", w którym zapisano – *„Rozbudowany katalog zadań inspektora ochrony danych wymaga, by taka osoba posiadała fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych osobowych. Pamiętaj, by odpowiedzialnie wybierać osoby, którym powierzysz zadania inspektora ochrony danych, sprawdzając stopień ich przygotowania do pełnienia tej funkcji, posiadaną wiedzę, praktyczne umiejętności oraz doświadczenie."*

Niestety nie podano kryteriów, według których to sprawdzanie powinno się odbywać.

Jedynym skutecznym rozwiązaniem przedstawionych powyżej problemów wydaje się być wprowadzenie mechanizmu obiektywnej zewnętrznej certyfikacji w tym zakresie.

Jednolity program certyfikacji, oparty o uporządkowane wymagania w stosunku do kandydatów, ale też wiedzy, którą powinni posiadać, stanowi szansę na ustandaryzowanie tego rynku a przede wszystkim na stworzenie wiarygodnego sposobu potwierdzania kompetencji Inspektorów.

DEKRA Certification Sp. z o.o. posiada ponad 16-letnie doświadczenie w obszarze certyfikacji. Program certyfikacji został opracowany i jest monitorowany przy udziale ekspertów z przedmiotowego zakresu. Kompetentni egzaminatorzy i doświadczony personel jednostki certyfikującej czuwają nad prawidłowym przebiegiem procesu.

Dzięki 3 letniej ważności certyfikatu i konieczności jego odnowienia dla utrzymania poświadczenia kwalifikacji, inspektorzy będą zobowiązani do stałego doskonalenia umiejętności, co zapewnia trwałość wymagań i potwierdzenie rzetelności procesu certyfikacji.

Zweryfikowane kadry, zajmujące się ochroną danych osobowych, przyczynią się do zwiększenia bezpieczeństwa danych, minimalizując ryzyko wystąpienia poważnych incydentów w tym obszarze. W efekcie program pozwoli uniknąć szkody dla bezpieczeństwa danych, a w konsekwencji dla gospodarki krajowej.

2. Skróty i terminologia

- Certyfikat - dokument wydany przez JCO zgodnie z postanowieniami normy PN-EN ISO/IEC 17024:2012, wskazujący, że wymieniona osoba spełnia wymagania certyfikacyjne
- RODO - ROZPORZĄDZENIE 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 (ogólne rozporządzenie o ochronie danych)

- Menedżer ds. Usług Ochrony Danych (Menedżer) – pracownik JCO odpowiedzialny za prowadzenie i nadzorowanie procesów związanych ze świadczonymi usługami certyfikacji osób
- Wnioskodawca/kandydat – osoba ubiegająca się o certyfikat, która spełnia wyspecyfikowane warunki wstępne certyfikacji
- Egzaminator – osoba posiadająca kompetencje do przeprowadzenia i podania oceny wyników egzaminu, gdy w ramach tego egzaminu wymagany jest profesjonalny osąd; do 7 osób egzaminowanych – jedna osoba, powyżej 7 egzaminowanych w jednym czasie – powołany przez JCO egzaminator oraz pomocnik egzaminatora
- Kompetencja - zdolność wykorzystania wiedzy i umiejętności do osiągnięcia zamierzonych wyników
- Ocena – proces porównania spełniania przez wnioskodawcę wymagań zawartych w programie certyfikacji
- Odwołanie – wystąpienie wnioskodawcy o ponowne rozpatrzenie negatywnej decyzji podjętej w procesie certyfikacji
- Pomocnik egzaminatora – pracownik JCO, przeszkolony z zasad przeprowadzania egzaminów
- Proces certyfikacji - działania, łącznie z wnioskowaniem, oceną, decyzją w sprawie certyfikacji, nadzorem, ponownej certyfikacji i wykorzystaniem certyfikatów oraz logo/znaków, za pomocą których jednostka certyfikująca ustala, że dana osoba spełnia wymagania certyfikacyjne.
- Program certyfikacji - określone wymagania certyfikacyjne i zasady prowadzenia tego procesu odnoszące się do kategorii osób, w stosunku do których stosuje się te same normy i zasady oraz te same procedury
- System certyfikacji – ogół procedur i zasobów do prowadzenia procesu certyfikacji

IOD	Inspektor Ochrony Danych
JCO	Jednostka Certyfikująca Osoby
DEKRA Certification	DEKRA Certification Sp. z o.o.
VA	Procedura
AA	Instrukcja
GF	Zarząd firmy
MSR	Pełnomocnik ds. zarządzania (aktualnie obowiązki pełni Szef Zespołu ZZ)
ZZ	Zespół Zarządzania i Certyfikacji
ZM	Zespół Marketingu i Rozwoju Biznesu
ZF	Zespół Finansów,
ZA	Zespół Administracji
MR	Menedżer Regionalny
MOD	Menedżer ds. Usług Ochrony Danych
OWCO	Ogólne Warunki Certyfikacji Osób

3. Powołania Normatywne

PN-EN ISO/IEC 17024:2012 Ocena zgodności. Ogólne wymagania dotyczące jednostek certyfikujących osoby.

ROZPORZĄDZENIE 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 (ogólne rozporządzenie o ochronie danych)

4. Zakres stosowania

Niniejszy program certyfikacji ma zastosowanie w procesie certyfikacji wnioskodawców na Inspektorów Ochrony Danych. Określają one wymagania zgodne z obowiązującymi przepisami, normami i specyfikacjami w ramach zakresu akredytacji, których spełnienie jest niezbędne na poszczególnych etapach procesu.

5. Opis procesu certyfikacji

Wniosek o certyfikację osób.
Proces certyfikacji rozpoczyna się w momencie złożenia w JCO przez kandydata wniosku o certyfikację osób. Do wniosku wnioskodawca powinien dołączyć kopię dokumentu poświadczającego ukończenie szkolenia w zakresie przedmiotowym certyfikacji. Wraz ze złożeniem wniosku kandydat przesyła ponadto podpisane Ogólne Warunki Certyfikacji Osób (OWCO).
Pierwszym etapem oceny jest weryfikacja złożonego wniosku przez Menedżera.
Menedżer, bądź osoba przez niego wyznaczona, sprawdza kompletność wniosku i załączników oraz prawidłowość ich wypełnienia. Po sprawdzeniu kompletności wniosku i weryfikacji informacji w nim zawartych, Menedżer dokonuje kwalifikacji wnioskodawcy poprzez sprawdzanie spełnienia przez wnioskodawcę wymagań.
W procesie kwalifikacji kandydatów Menedżer może zwrócić się do Komitetu Technicznego o wydanie opinii.
Po pozytywnym zakwalifikowaniu wnioskodawcy, Menedżer bądź osoba wyznaczona dokonuje rejestracji kandydata w bazie i zakłada teczkę osobową wnioskodawcy. Wnioskujący otrzymuje potwierdzenie przyjęcia wniosku o certyfikację osób z kwalifikacją.
W przypadku negatywnego wyniku sprawdzenia Menedżer może wezwać wnioskującego o uzupełnienie brakujących dokumentów, bądź zawiadamia wnioskującego o nieścisłościach. Rejestracja wnioskodawcy w bazie następuje w dniu usunięcia nieścisłości.
Wniosek o certyfikację osób, wraz z załącznikami stanowi umowę pomiędzy wnioskodawcą a JCO na przeprowadzenie procesu certyfikacji.

Wymagania względem wnioskodawców, a następnie ocena i decyzja o przyznaniu certyfikatu odnosi się wyłącznie do procesu certyfikacji.

Wymagania dla wnioskodawców ubiegających się o certyfikat IOD:

- Wykształcenie minimum średnie
- Doświadczenie zawodowe:
    - Przy wykształceniu wyższym:

      minimum 1 rok doświadczenia zawodowego w obszarze ochrony danych (przeprowadzanie audytów danych osobowych lub nadzorowanie przestrzegania przepisów w zakresie danych osobowych w ramach pełnienia funkcji ABI/IOD lub podobnej (np. specjalista ds. ochrony danych) lub w ramach obszaru doradztwa ABI/IOD w zakresie ochrony danych osobowych). Dodatkowym atutem jest doświadczenie w zakresie audytowania, nadzorowania (np. pełnienie roli Pełnomocnika SZBI, Oficera Bezpieczeństwa) lub doradzania systemów bezpieczeństwa informacji wg. ISO 27001.

DEKRA Certification Sp. z o.o., ul. Legnicka 48H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

- Przy wykształceniu średnim:

  minimum 3 lata doświadczenia zawodowego w obszarze ochrony danych (przeprowadzanie audytów danych osobowych, lub nadzorowanie przestrzegania przepisów w zakresie danych osobowych w ramach pełnienia funkcji ABI/IOD lub podobnej (np. specjalista ds. ochrony danych) lub w ramach obszaru doradztwa ABI/IOD w zakresie ochrony danych osobowych). Dodatkowym atutem jest doświadczenie w zakresie audytowania, nadzorowania (np. pełnienie roli Pełnomocnika SZBI, Oficera Bezpieczeństwa) lub doradzania systemów bezpieczeństwa informacji wg. ISO 27001.

- Ukończone szkolenia/kursy w zakresie ochrony danych osobowych w wymiarze łącznym co najmniej 16 godzin lub ukończone studia podyplomowe w obszarze ochrony danych osobowych – w zakresie odpowiadającym ramowemu programowi szkolenia JCO.

Poza powyższymi wymaganiami JCO nie stawia żadnych dodatkowych wymagań np. dotyczących przynależności do stowarzyszeń oraz innych utrudniających dostęp do egzaminu.

Ocena

Zasadniczym etapem oceny jest egzamin sprawdzający kompetencje i wiedzę wnioskodawcy.

Egzamin jest pisemny.
Na potrzeby egzaminów tworzona jest pula pytań egzaminacyjnych. Pula pytań przechowywana jest w sposób uniemożliwiający niepowołany dostęp do puli osób trzecich. Menedżer minimum raz w roku i każdorazowo w przypadku zmiany wymagań prawnych dokonuje przeglądu i aktualizacji puli pytań.

Egzamin pisemny składa się z 30 pytań jednokrotnego wyboru oraz 3 pytań otwartych, wymagających analizy sytuacyjnej konkretnego problemu. Egzamin trwa 90 minut. Nadzór nad egzaminem prowadzi Egzaminator.

Egzaminy są przeprowadzane w odpowiednich salach, zorganizowanych w sposób zapewniający indywidualne odpowiadanie na pytania. Egzaminator otrzymuje zestawy pytań w zapieczętowanej kopercie i otwiera je dopiero po ogłoszeniu reguł egzaminacyjnych.

Oceny wyników dokonuje Egzaminator w sposób uczciwy, miarodajny i wiarygodny.

Egzamin składa się z:

- 30 zadań jednokrotnego wyboru. Każde zadanie wymaga od kandydata wybrania jednej prawidłowej odpowiedzi spośród kilku podanych w zadaniu. Za każde prawidłowo rozwiązane zadanie przyznawany jest jeden punkt. Maksymalna liczba punktów możliwych do uzyskania wynosi 30.
- oraz składa się z 3 pytań otwartych, wymagających analizy sytuacyjnej konkretnego problemu. Za poprawną analizę problemu i udzielenie odpowiedzi można uzyskać maksymalnie 10 punktów. Maksymalna liczba punktów możliwych do uzyskania wynosi 30.

Kryteria oceny pytań otwartych:

1. Znajomość przepisów o ochronie danych i przyporządkowanie sytuacji do przepisów RODO - max 2 punkty:

DEKRA Certification Sp. z o.o., ul. Legnicka 48H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

0 pkt – brak lub ograniczona znajomość wymagań prawnych. Brak lub w większości błędne odwołania do wymagań prawnych.
1 pkt - zadawalająca znajomość wymagań prawnych w odniesieniu do sytuacji. Właściwe odwołania do większości wymagań prawnych.
2 pkt – bardzo dobra znajomość wymagań prawnych w odniesieniu do sytuacji. Właściwe odwołania wszystkich wymagań prawnych. Zdający właściwie interpretuje wymagania prawne.

2. Prawidłowość oceny sytuacji w odniesieniu do obowiązków Inspektora Ochrony Danych (IOD) - max 2 punkty:
0 pkt – brak lub bardzo ograniczona umiejętność oceny sytuacji w odniesieniu do obowiązków IOD, brak prezentacji wyników w zadaniu, zdający nie wskazuje lub niewłaściwie identyfikuje rolę IOD w procesach przetwarzania danych osobowych.
1,5 pkt – zadawalająca umiejętność oceny sytuacji w odniesieniu do obowiązków IOD, przejrzysty sposób prezentacji wyników w zadaniu, zdający poprawnie identyfikuje rolę IOD w procesach przetwarzania danych osobowych.
2 pkt - bardzo dobra umiejętność oceny sytuacji w odniesieniu do obowiązków IOD, przejrzysty i kompleksowy sposób prezentacji wyników w zadaniu, zdający właściwie identyfikuje rolę IOD w procesach przetwarzania danych osobowych również w sytuacjach złożonych.

3. Prawidłowość rozwiązania problemu, łącznie max 4 punkty, z tego:
a. zrozumienie sytuacji - max 1 punkt:
0 pkt – brak lub bardzo ograniczone zrozumienie sytuacji, zdający niewłaściwie identyfikuje istotę poruszanych zagadnień
0,5 pkt – zadawalające zrozumienie sytuacji , zdający poprawnie identyfikuje istotę poruszanych zagadnień
1 pkt – bardzo dobre zrozumienie sytuacji, zdający właściwie identyfikuje istotę poruszanych zagadnień, również w sytuacjach złożonych .

b. rozpoznanie zagrożeń i ocena skutków - max 1 punkt:
0 pkt – brak lub bardzo ograniczone rozpoznanie zagrożeń i ocena, zdający niewłaściwie identyfikuje ryzyka.
0,5 pkt – zadawalające rozpoznanie zagrożeń i ocena, zdający poprawnie identyfikuje ryzyka.
1 pkt – bardzo dobre rozpoznanie zagrożeń i ocena, zdający właściwie identyfikuje ryzyka.

c. zastosowanie odpowiednich środków w odniesieniu do bezpieczeństwa technicznego i organizacyjnego – max. 2 punkty:
0 pkt – brak lub bardzo ograniczona umiejętność zastosowania odpowiednich środków w odniesieniu do bezpieczeństwa technicznego i organizacyjnego, zdający nie identyfikuje lub niewłaściwie identyfikuje wymagania w zakresie zabezpieczeń.
1 pkt – zadawalająca umiejętność zastosowania odpowiednich środków w odniesieniu do bezpieczeństwa technicznego i organizacyjnego, zdający poprawnie identyfikuje wymagania w zakresie zabezpieczeń.
2 pkt – bardzo dobra umiejętność zastosowania odpowiednich środków w odniesieniu do bezpieczeństwa technicznego i organizacyjnego, zdający właściwie identyfikuje wymagania w zakresie zabezpieczeń.

4. Wyjaśnienie / uzasadnienie sposobu postępowania - max 2 punkty:
0 pkt – zdający nie potrafi lub błędnie uzasadniania sposobu postepowania, a sformułowania są przeważnie nieadekwatne.
1,5 pkt – zdający zadawalająco uzasadniania sposobu postępowania, a sformułowania są adekwatne.

2 pkt - zdający właściwie i kompleksowo uzasadniania sposobu postępowania, a sformułowania są adekwatne

- Maksymalna liczba punktów możliwych do uzyskania z całego egzaminu wynosi 60.
- Aby zdać egzamin, uczestnik musi uzyskać łącznie minimum 46 punktów.

Decyzja
Decyzję o certyfikacji podejmowana jest na podstawie:
- zatwierdzonego przez Menedżera wniosku o certyfikację osób;
- dokumentów egzaminacyjnych.
Przebieg procesu podejmowania decyzji o certyfikacji opisany jest w procedurze V-09SS-x03pl Przebieg procesu certyfikacji osób.

Certyfikat wydawany jest na okres 3 lat. Certyfikat powinien zawierać co najmniej:
a) imię i nazwisko osoby, która uzyskała dany certyfikat;
b) datę uzyskania certyfikatu;
c) datę upływu okresu ważności certyfikatu;
d) zakres certyfikacji;
e) nazwę jednostki certyfikującej;
f) numer identyfikacyjny;
g) podpisy osób reprezentujących jednostkę certyfikującą.
h) powołanie się na program certyfikacji

Decyzje o wyniku procesu certyfikacji przekazywane są wnioskującemu pisemnie.

Od decyzji Komitetu Technicznego przysługuje wnioskującemu odwołanie, zgodnie z V-013-x01pl Odwołania i skargi – postępowanie.

Ponowna certyfikacja

JCO na wniosek posiadacza certyfikatu, dwa miesiące przed upływem ważności certyfikatu może udzielić nowego certyfikatu na kolejne trzy lata, po weryfikacji dokumentacji, wskazującej na spełnienie wymagań dotyczących utrzymania kompetencji. Warunkiem ponownej certyfikacji jest:

- Wykazanie przez osobę certyfikowaną co najmniej rocznego doświadczenia w obszarze ochrony danych osobowych
- Ukończone szkolenia/kursy w zakresie danych osobowych w wymiarze łącznym co najmniej 16 godzin lub ukończone studia podyplomowe,

w okresie ważności certyfikatu.
Odnowienie certyfikatu następuje po 3 latach.

Cofnięcie certyfikatu

DEKRA Certification Sp. z o.o. jako Jednostka Certyfikująca Osoby uprawniona jest w każdym momencie do cofnięcia certyfikatu DEKRA, jeżeli:

- warunki przyznania certyfikatu nie są (już) spełnione, na przykład ze względu na podanie niekompletnych lub nieprawdziwych danych w procedurze certyfikacyjnej;

- niespełnienie wymagań postawionych przez jednostkę certyfikacyjną w okresie zawieszenia certyfikatu kompetencji

DEKRA Certification Sp. z o.o., ul. Legnicka 48H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

- wystąpią inne przyczyny uprawniające do cofnięcia certyfikatu na podstawie OWCP.

W przypadku cofnięcia certyfikatu, uzyskanie certyfikatu wymaga ponownej certyfikacji.

Zawieszenie certyfikatu

DEKRA Certification Sp. z o.o. uprawniona jest w każdym momencie do zawieszenia certyfikatu DEKRA w przypadku:

- zgłoszenia przez osobę certyfikowaną czasowej rezygnacji z certyfikatu
- gdy osoba certyfikowana lub zleceniodawca, tj. podmiot delegujący pracownika do procesu certyfikacji, nie dopełniają obowiązków nałożonych na nich w związku z certyfikacją, na przykład obowiązku informowania o zmianach, lub nie spełniają zobowiązań wynikających z umowy zawartej z DEKRA Certification Sp. z o. o. w szczególności zobowiązań dotyczących płatności;
- gdy przedmiot użytkowania, na przykład certyfikat DEKRA, wykorzystywany będzie niezgodnie z warunkami użytkowania, określonymi w OWCP;
- stwierdzenia przekroczenia uprawnień, wynikających z przyznanego certyfikatu lub mających na celu świadome wprowadzenie w błąd
- niespełnienia wymagań określonych przez jednostkę certyfikującą, stwierdzonego w okresie ważności certyfikatu.

6. Prawa i obowiązki wnioskodawcy i osoby certyfikowanej

Kandydat do certyfikacji ma prawo do:
- żądania wglądu do dokumentacji z przebiegu swojego procesu certyfikacji.
- wniesienia skargi/odwołania na przebieg procesu certyfikacji po otrzymaniu decyzji z każdego etapu procesu
- oceny egzaminu i egzaminatora
- złożenia zastrzeżenia do osoby egzaminatora (przed egzaminem)
- rezygnacji z przystąpienia do egzaminu
- korzystania z dozwolonych pomocy podczas egzaminu (RODO).

Kandydat do certyfikacji ma obowiązek:
- zastosowania się do przedstawionych warunków przeprowadzania egzaminu
- samodzielnej pracy podczas egzaminu.

Osoba certyfikowana zobowiązana jest do spełniania warunków przyznania certyfikatu i do niezwłocznego informowania DEKRA Certification o wszelkich zmianach mogących mieć wpływ na spełnienie warunków utrzymania certyfikatu.

7. Prawa i obowiązki JCO

Obowiązkiem JCO jest sprawowanie nadzoru nad prawidłowością stosowania certyfikatu.

JCO zobowiązana jest do powiadamiania posiadacza certyfikatu o zmianach w systemie certyfikacji oraz zmianach przepisów prawnych i norm dotyczących certyfikatu w okresie jego ważności. Zmiany te będą przesyłane posiadaczom certyfikatów w formie informacji drogą elektroniczną.

JCO ma obowiązek przechowywać i nadzorować dokumentację dotyczącą wnioskodawcy i osoby certyfikowanej, a także dokumentację z przebiegu certyfikacji, w warunkach zapewniających ochronę danych, bezpieczeństwo i poufność.

Jednostka certyfikująca przechowuje i nadzoruje, dokumentację dotyczącą każdej osoby, która otrzymała certyfikat oraz dokumentację z przebiegu procesu certyfikacji.
Dokumentacja dotycząca poszczególnych osób jest przechowywana w warunkach zapewniających bezpieczeństwo i poufność. Dane dotyczące przebiegu procesu certyfikacji i nadzoru rejestrowane są również w bazie.

8. Wymagania w zakresie kompetencji oraz zadań i odpowiedzialności IOD

Do zadań IOD zgodnie z art. 39 RODO należą w szczególności:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;.
- udzielanie zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonywania;
- monitorowanie przestrzegania rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- współpraca z organem nadzorczym;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach w obszarze ochrony danych.

Wymagania kompetencyjne dla osoby pełniącej funkcję IOD:

- wiedza fachowa w zakresie prawa i praktyk w dziedzinie ochrony danych
- podstawowa znajomość zagadnień bezpieczeństwa systemów informatycznych
- sumienność, rzetelność i odpowiedzialność w wykonywaniu zadań.

Zasady postępowania certyfikowanego Inspektora Ochrony Danych:

- Certyfikowany Inspektor Ochrony Danych jest sumiennie realizuje powierzone zadania.

- Certyfikowany IOD realizuje swoje zadania w sposób niezależny i nie przyjmuje instrukcji w zakresie sposobu realizacji działań.
- Certyfikowany IOD może realizować inne zadania pod warunkiem, że zadania te nie powodują konfliktu interesów.
- Certyfikowany IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.
- Certyfikowany IOD dba o utrzymanie kwalifikacji oraz wysokiego poziomu fachowej wiedzy na temat prawa i praktyk z dziedziny ochrony danych.

9. Wymagania dla jednostek szkoleniowych (trenerzy, programy szkoleniowe, organizacja)

DEKRA Certification nie prowadzi szkoleń z zakresu objętego programem certyfikacji.

Jednostka prowadząca szkolenia dla IOD powinna wyznaczyć osobę odpowiedzialną za ogólne zarządzanie szkoleniami, która będzie czuwała nad jakością świadczonych usług szkoleniowych oraz kompetencjami trenerów.
Jednostka prowadząca szkolenia dla IOD powinna ponadto mieć określone wymagania kompetencyjne dla trenerów.
Ponadto jednostka powinna zapewnić monitorowanie jakości prowadzonych szkoleń.
Obowiązkiem jednostki prowadzącej szkolenia dla IOD jest zapewnienie uczestnikom szkoleń informacji o warunkach uczestnictwa w szkoleniu, programie szkolenia i kwestiach organizacyjnych.

Jednostka prowadząca szkolenia powinna prowadzić dokumentację z przeprowadzonych szkoleń wraz z rejestrem wydanych Zaświadczeń ze szkolenia.

Program szkolenia powinien określać m.in. cel szkolenia, jego zakres tematyczny, oraz jego plan. Program szkolenia musi być zgodny z programem określonym przez JCO – załącznik nr 1 do Umowy z firma szkoleniową. Każdy uczestnik szkolenia powinien otrzymać pełen zestaw materiałów szkoleniowych.

Uznane przez DEKRA Certification jednostki szkoleniowe wymienione są na naszej stronie internetowej.

Jednocześnie JCO akceptuje wnioski wnioskodawców, którzy ukończyli szkolenia w innych jednostkach szkoleniowych pod warunkiem, że szkolenie to spełnia warunki ramowego programu szkolenia IOD DEKRA Certification.

10. Kwalifikacje i powołanie egzaminatorów

Wszyscy egzaminatorzy są powoływani przez Zarząd DEKRA Certification lub przez Menedżera.
Powoływanie egzaminatorów w DEKRA Certification odbywa się w oparciu o przedstawione kwalifikacje oraz możliwość spełnienia określonych funkcji.
Wymagania w stosunku do egzaminatorów:

- Wykształcenie wyższe
- Doświadczenie zawodowe:

DEKRA Certification Sp. z o.o., ul. Legnicka 48H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

- Przy wykształceniu wyższym min. 2 lata doświadczenia zawodowego w obszarze ochrony danych osobowych (przeprowadzanie audytów danych osobowych uwzględniających zagadnienia prawne, organizacyjne i techniczne lub nadzorowanie przestrzegania przepisów w zakresie danych osobowych w ramach pełnienia funkcji ABI/IOD lub w ramach obszaru doradztwa w obszarze ochrony danych osobowych (przeprowadzanie audytów danych osobowych uwzględniających zagadnienia prawne, organizacyjne i techniczne lub nadzorowanie przestrzegania przepisów w zakresie danych osobowych w ramach pełnienia funkcji ABI/IOD lub w ramach obszaru doradztwa w zakresie ochrony danych osobowych z uwzględnieniem wymagań prawnych).

- Ukończone i nie starsze niż 5 lat szkolenia/kursy w zakresie ochrony danych osobowych w łącznym wymiarze co najmniej 24 godzin lub ukończone studia podyplomowe w zakresie ochrony danych lub prowadzenie szkoleń/kursów w zakresie ochrony danych w łącznym wymiarze co najmniej 40 godzin.

- Dodatkowym atutem jest doświadczenie w zakresie audytowania, nadzorowania (np. pełnienie roli Pełnomocnika SZBI, Oficera Bezpieczeństwa) lub doradzania systemów bezpieczeństwa informacji wg. ISO 27001.

Warunkiem nawiązania współpracy z egzaminatorem jest podpisanie dokumentu D-06S-x09pl Warunki przeprowadzania egzaminów w ramach certyfikacji osób.

Powołanie na egzaminatora udzielane jest na 3 lata, na podstawie wypełnionego profilu zawodowego. W tym czasie obowiązkowo musi być przeprowadzony przynajmniej 1 monitoring egzaminatora. Powołanie może zostać przedłużone na kolejne trzy lata. Warunkiem utrzymania statusu egzaminatora jest przeprowadzenie przez niego min. 1 egzaminu oraz pozytywna ocena z monitoringu, dokonanego przez Menedżera lub osobę przez niego wyznaczoną.

W czasie trwania powołania, egzaminator jest zobowiązany raz w roku uczestniczyć w wymianie doświadczeń dla egzaminatorów. Ponadto egzaminator zobowiązany jest do odbycia co najmniej jednego szkolenia/kursu w wymiarze 8 godzin lub udziału w konferencji o tematyce ochrony danych.

Na 3-4 miesiące przed datą wygaśnięcia ważności powołania Egzaminator jest informowany o upływie jego ważności. Egzaminator proszony jest o przesłanie zaktualizowanego profilu zawodowego wraz z załącznikami o utrzymaniu kwalifikacji.
Wznowienie powołania następuje najpóźniej na 4 tygodnie przed upływem daty ważności poprzedniego powołania - data ważności poprzedniego powołania zostaje przedłużona o kolejne 3 lata

Szczegółowa procedura powoływania egzaminatorów znajduje się w dokumencie V-09SS-x03pl Przebieg procesu certyfikacji osób.

11. Załączniki

- Załącznik 1 – umowa z firmą szkoleniową

Umowa nr …….

zawarta w dniu ……... pomiędzy:

DEKRA Certification Sp. z o.o. z siedzibą we Wrocławiu, Legnicka 48 H, 54-202 Wrocław

wpisaną do Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Wrocławia-Fabrycznej, VI wydział Gospodarczy; numer KRS 0000010810;

NIP 899-24-08-842, którą reprezentują:

1.

2.

zwaną dalej **DEKRA Certification,**

a

……..

z siedzibą w ……..., wpisaną do Krajowego Rejestru Sądowego w Sądzie ……. pod numerem KRS …….

którą reprezentuje:

……

zwaną dalej **…….**

§ 1 Postanowienia ogólne

1. Przedmiotem umowy jest ustalenie zasad i warunków współpracy pomiędzy DEKRA Certification a ……..
2. Strony deklarują współpracę w zakresie propagowania idei podnoszenia i potwierdzania kwalifikacji osób poprzez certyfikację.
3. Umawiające się strony nie są upoważnione do przekazywania praw i obowiązków wynikających z tej umowy na podmioty trzecie, bez wcześniejszej pisemnej zgody drugiej strony.
4. Strony nie mają prawa żądania od siebie wzajemnie jakiegokolwiek wynagrodzenia z tytułu realizacji niniejszej umowy.

§ 2 Zobowiązania stron

1. ……. przygotuje materiały szkoleniowe dla kandydatów do certyfikacji oraz programy szkolenia zgodnie z ramowymi wytycznymi, ujętymi w załączniku nr 1 do niniejszej umowy.

2. …….. jest organizatorem szkoleń otwartych realizowanych w ramach niniejszej umowy.
3. DEKRA Certification ma prawo wglądu do programu i materiałów, o których mowa w ust. 1 przed podpisaniem niniejszej umowy oraz po każdej zmianie dokonanej w tych programach i materiałach. Ponadto …… zobowiązuje się udostępnić program i materiały na każde żądanie DEKRA Certification. Ograniczenie możliwości wglądu może być podstawą rozwiązania niniejszej umowy.
4. DEKRA Certification dopuszcza do egzaminów kandydatów, którzy odbyli szkolenie w …… według programów i z udziałem materiałów, o których mowa w ust. 1 i 3, pod warunkiem spełniania przez kandydatów pozostałych wymagań dopuszczających do udziału w egzaminie.
5. DEKRA Certification przeprowadza egzaminy w oparciu o program certyfikacji w zakresie, którego dotyczą szkolenia, opisane w załączniku.
6. ……. zobowiązuje się do zlecania prowadzenia szkoleń, określonych w załączniku nr 1 wyłącznie ekspertom o wysokich kwalifikacjach, gwarantujących wysoki poziom prowadzonych szkoleń, wpisanym do bazy kwalifikowanych trenerów-ekspertów ……...
7. DEKRA Certification i …… zobowiązują się do zachowania w tajemnicy wszystkiego, co wiąże się ze wzajemną współpracą w ramach niniejszej umowy, w szczególności przekazanych materiałów i informacji oraz treści niniejszej umowy. Zobowiązanie to obowiązuje w czasie trwania Umowy i po jej zakończeniu. Na stronach ciąży zobowiązanie do tego samego swoich pracowników.
8. Strony wyrażają zgodę na przekazanie materiałów marketingowych swoim klientom, w szczególności broszur informacyjnych dotyczących ich działalności.

§ 3 Zawiązanie i rozwiązanie Umowy

1. Umowa wchodzi w życie z dniem jej podpisania przez obydwie strony.
2. Umowę zawarto na czas nieokreślony.
3. Każdej ze stron przysługuje prawo rozwiązania umowy w każdym czasie za wypowiedzeniem. Okres wypowiedzenia wynosi 3 miesiące.
4. W przypadku naruszenia postanowień niniejszej umowy każda ze stron ma prawo rozwiązać umowę w trybie natychmiastowym, bez zachowania okresu wywiedzenia, po uprzednim pisemnym wezwaniu drugiej strony do zaprzestania naruszeń w terminie 7 dni i niezastosowaniu się przez drugą stronę do powyższego wezwania.
5. Umowa może być rozwiązana przez każdą ze stron ze skutkiem natychmiastowym, bez zachowania okresu wypowiedzenia w przypadkach:
    a. dokonania zmian w programach i materiałach szkoleniowych o których mowa w §2 ust. 1 i 3 bez pisemnego poinformowania i akceptacji DEKRA Certification,
    b. naruszenia zasad dotyczących konkurencji,
    c. złamania zasady zachowania tajemnicy,
    d. narażenia dobrego imienia lub wizerunku jednej ze stron Umowy,
    e. niedotrzymania warunków określonych w Umowie.

DEKRA Certification Sp. z o.o., ul. Legnicka 48H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

6. Wypowiedzenie umowy nie zwalnia stron z obowiązku ukończenia prac, zleceń i wywiązania się ze zobowiązań podjętych przed dokonaniem wypowiedzenia przez jedną ze stron, w szczególności w sytuacji, gdy zobowiązania te dotyczą osób i podmiotów trzecich.
7. Rozwiązanie umowy pomiędzy stronami nie ma wpływu na ważność wystawionych przez DEKRA Certification certyfikatów i zaświadczeń.
8. W przypadku wypowiedzenia umowy przez którąkolwiek ze stron, strony zobowiązane są do zwrotu wszystkich powierzonych wzajemnie wydawnictw, materiałów roboczych, metodologii i innej dokumentacji. Strony nie mają prawa do wykonywania jakichkolwiek kopii, magazynowania na nośnikach magnetycznych, systemach komputerowych i innych, a także do przekazywania innym osobom, instytucjom, etc. ww. dokumentów.

§ 4 Postanowienia końcowe

1. Podpisanie niniejszej umowy przez strony unieważnia wszelkie wcześniejsze ustalenia poczynione w jakiejkolwiek formie.
2. Strony zobowiązują się do rozstrzygania wszystkich sporów w sposób polubowny.
3. Sądem miejscowo właściwym dla rozstrzygania sporów wynikających z umowy jest sąd właściwy dla siedziby DEKRA Certification.
4. Niniejsza umowa może zostać zmieniona przez strony z zachowaniem formy pisemnej pod rygorem nieważności.
5. Strony nie dokonały żadnych ubocznych ustaleń ustnych zmieniających treść niniejszej umowy.
6. Do rozwiązania niniejszej umowy wystarczy przesłanie listem poleconym stosownego pisma. Jako wiążącą uznaje się datę stempla pocztowego.
7. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

....

DEKRA Certification Sp. z o.o.

DEKRA Certification Sp. z o.o., ul. Legnicka 48H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

Zał. Nr 1 do umowy nr ……..

Jednostka prowadząca szkolenia:

- wyznacza osobę odpowiedzialną za ogólne zarządzanie szkoleniami, która będzie czuwała nad jakością świadczonych usług
- określa wymagania kompetencyjne dla trenerów
- monitoruje jakość prowadzonych szkoleń
- prowadzi dokumentacje ze szkoleń wraz z rejestrem uczestników
- prowadzi szkolenia odpowiadające ramowemu programowi:

Ramowy Program szkolenia w zakresie ochrony danych osobowych

LP	TEMAT	Czas teoria (h)	Czas ćwiczenia (h)
1.	Podstawy prawne ochrony danych osobowych na poziomie europejskim i krajowym	10	6
2.	Prawo cywilne (w zakresie dotyczącym danych osobowych)		
3.	Definicje w zakresie ochrony danych osobowych		
4.	Zasady dot. przetwarzania danych osobowych		
5.	Prawa osoby, której dane dotyczą		
6.	Obowiązki administratora danych osobowych		
7.	Przetwarzanie danych osobowych w imieniu administratora		
8.	Bezpieczeństwo danych osobowych (informatyczne, techniczne, organizacyjne)		
9.	Zagadnienia w zakresie zagrożeń bezpieczeństwa danych (zagrożenia cybernetyczne, fizyczne, etc.)		
10.	Ocena skutków dla ochrony danych/szacowanie ryzyka		
11.	Inspektor Ochrony Danych (wyznaczenie, status, zadania)		
12.	Dokumentacja przetwarzania danych		
13.	Transfer danych do państw trzecich		
14.	Zagadnienia dot. postępowania przy naruszeniu ochrony danych osobowych		
15.	Zagadnienia dot. kontroli, audytu i certyfikacji		
16.	Środki ochrony prawnej, odpowiedzialność i sankcje		
	RAZEM:	10	6

DEKRA Certification Sp. z o.o., ul. Legnicka 48H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/