Rada
Unii Europejskiej

Bruksela, 16 września 2022 r.
(OR. en)

Międzyinstytucjonalny numer referencyjny:
2022/0272(COD)

12429/22
ADD 1

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	15 września 2022 r.
Do:	Sekretariat Generalny Rady
Nr dok. Kom.:	COM(2022) 454 final - Annexes
Dotyczy:	ZAŁĄCZNIKI do WNIOSKU DOTYCZĄCEGO ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020

Delegacje otrzymują w załączeniu dokument COM(2022) 454 final - Annexes.

Zał.: COM(2022) 454 final - Annexes

KOMISJA
EUROPEJSKA

Bruksela, dnia 15.9.2022 r.
COM(2022) 454 final

ANNEXES 1 to 6

ZAŁĄCZNIKI

do

WNIOSKU DOTYCZĄCEGO ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

ZAŁĄCZNIK I

ZASADNICZE WYMOGI CYBERBEZPIECZEŃSTWA

1. WYMOGI BEZPIECZEŃSTWA DOTYCZĄCE CECH PRODUKTÓW Z ELEMENTAMI CYFROWYMI

1) Produkty z elementami cyfrowymi należy projektować, opracowywać i produkować w taki sposób, aby zapewniały odpowiedni poziom cyberbezpieczeństwa w zależności od ryzyka.

2) Produkty z elementami cyfrowymi należy dostarczać bez żadnych znanych i możliwych do wykorzystania podatności.

3) Na podstawie oceny ryzyka, o której mowa w art. 10 ust. 2, i w stosownych przypadkach produkty z elementami cyfrowymi:

   a) należy dostarczać wraz z bezpieczną konfiguracją domyślną, w tym z możliwością zresetowania produktu, tak aby przywrócić go do stanu pierwotnego;

   b) muszą zapewniać ochronę przed nieuprawnionym dostępem za pomocą odpowiednich mechanizmów kontroli, w tym między innymi systemów uwierzytelniania, identyfikacji lub zarządzania dostępem;

   c) muszą zapewniać ochronę poufności przechowywanych, przekazywanych lub w inny sposób przetwarzanych danych, w tym danych osobowych lub innych, np. przez szyfrowanie odpowiednich danych odłożonych lub danych przesyłanych z wykorzystaniem najnowocześniejszych mechanizmów;

   d) muszą zapewniać ochronę integralności przechowywanych, przekazywanych lub w inny sposób przetwarzanych danych, w tym danych osobowych lub innych, komend, programów i konfiguracji przed wszelką manipulacją lub modyfikacją nieautoryzowaną przez użytkownika, a także powiadamiać o uszkodzeniach;

   e) mogą przetwarzać wyłącznie dane, w tym dane osobowe lub inne, które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne w związku z przeznaczeniem produktu („minimalizacja danych”);

   f) muszą zapewniać ochronę dostępności podstawowych funkcji, w tym odporność na ataki typu „odmowa usługi” i łagodzenie ich skutków;

   g) muszą minimalizować własny negatywny wpływ na dostępność usług dostarczanych przez inne urządzenia lub sieci;

   h) należy projektować, opracowywać i produkować w taki sposób, aby ograniczyć powierzchnię ataku, w tym interfejsów zewnętrznych;

   i) należy projektować, opracowywać i produkować w taki sposób, aby zmniejszyć wpływ incydentu przy użyciu odpowiednich mechanizmów i technik łagodzenia skutków wykorzystania;

   j) muszą dostarczać informacji związanych z bezpieczeństwem przez rejestrowanie lub monitorowanie odpowiedniej aktywności wewnętrznej, w tym dostępu do danych, usług lub funkcji lub ich modyfikacji;

k) muszą zapewniać możliwość eliminowania podatności przez aktualizacje zabezpieczeń, w tym, w stosownych przypadkach, dzięki aktualizacjom automatycznym i powiadamianiu użytkowników o dostępnych aktualizacjach.

2. WYMOGI DOTYCZĄCE POSTĘPOWANIA W PRZYPADKU WYKRYCIA PODATNOŚCI

Producenci produktów z elementami cyfrowymi mają obowiązek:

1) identyfikowania i dokumentowania podatności i komponentów zawartych w produkcie, w tym przez sporządzenie zestawienia podstawowych materiałów do produkcji oprogramowania w powszechnie używanym formacie nadającym się do odczytu maszynowego, obejmującego co najmniej zależności najwyższego poziomu produktu;

2) w odniesieniu do ryzyka, jakie stwarzają produkty z elementami cyfrowymi – bezzwłocznego odpowiadania na podatności i ich eliminowania, w tym przez udostępnianie aktualizacji zabezpieczeń;

3) przeprowadzania skutecznych i regularnych testów i przeglądów bezpieczeństwa produktu z elementami cyfrowymi;

4) po udostępnieniu aktualizacji zabezpieczeń – publicznego ujawniania informacji o naprawionych podatnościach, w tym opisu podatności, informacji pozwalających użytkownikom zidentyfikować produkt z elementami cyfrowymi, którego te podatności dotyczą, skutków podatności, ich dotkliwości oraz informacji pomagających użytkownikom wyeliminować podatności;

5) wprowadzania i egzekwowania polityki skoordynowanego ujawniania podatności;

6) przyjmowania środków ułatwiających wymianę informacji o potencjalnych podatnościach w ich produkcie z elementami cyfrowymi, a także w komponentach strony trzeciej zawartych w tym produkcie, w tym przez udostępnienie adresu do kontaktu służącego do zgłaszania podatności wykrytych w produkcie z elementami cyfrowymi;

7) zapewniania mechanizmów bezpiecznej dystrybucji aktualizacji produktów z elementami cyfrowymi w celu zapewnienia, aby możliwe do wykorzystania podatności zostały naprawione lub ograniczone w odpowiednim czasie;

8) zapewniania, aby w przypadku gdy dostępne są poprawki lub aktualizacje zabezpieczeń służące rozwiązaniu zidentyfikowanych problemów bezpieczeństwa, były one rozpowszechniane bezzwłocznie i bezpłatnie, wraz z komunikatami doradczymi dostarczającymi użytkownikom odpowiednich informacji, w tym na temat potencjalnych działań, które należy podjąć.

ZAŁĄCZNIK II

INFORMACJE I INSTRUKCJE DLA UŻYTKOWNIKÓW

Produktowi z elementami cyfrowymi muszą towarzyszyć co najmniej następujące informacje:

1. imię i nazwisko lub nazwa, zarejestrowana nazwa handlowa lub zarejestrowany znak towarowy producenta oraz adres pocztowy i adres e-mail, pod którym można się skontaktować z producentem, umieszczone na produkcie albo – jeżeli nie jest to możliwe – na opakowaniu produktu lub w załączonym do niego dokumencie;
2. punkt kontaktowy, w którym można zgłosić i otrzymać informacje o podatnościach produktu wpływających na cyberbezpieczeństwo;
3. poprawne określenie typu, partii, wersji lub numeru seryjnego lub innego elementu umożliwiającego identyfikację produktu oraz odpowiednie instrukcje i informacje dla użytkowników;
4. przeznaczenie, w tym środowisko bezpieczeństwa zapewnione przez producenta, a także zasadnicze funkcje produktu i informacje o zabezpieczeniach;
5. wszelkie znane lub dające się przewidzieć okoliczności związane z wykorzystaniem produktu z elementami cyfrowymi zgodnie z jego przeznaczeniem lub w warunkach racjonalnie przewidywalnego niewłaściwego wykorzystania, które mogą powodować znaczące ryzyko w cyberprzestrzeni;
6. wskazanie, czy można uzyskać dostęp do zestawienia podstawowych materiałów do produkcji oprogramowania, a jeśli tak, to gdzie;
7. w stosownych przypadkach adres strony internetowej, na której jest dostępna deklaracja zgodności UE;
8. określenie rodzaju wsparcia technicznego w zakresie bezpieczeństwa oferowanego przez producenta oraz do kiedy będzie ono udzielane, a co najmniej do kiedy użytkownicy mogą spodziewać się otrzymania aktualizacji zabezpieczeń;
9. szczegółowe instrukcje lub adres strony internetowej odsyłający do takich szczegółowych instrukcji oraz informacji na temat:
    a) środków niezbędnych podczas pierwszego uruchomienia oraz przez cały okres życia produktu w celu zapewnienia jego bezpiecznego użytkowania;
    b) wpływu, jaki zmiany w produkcie mogą mieć na bezpieczeństwo danych;
    c) sposobu instalowania aktualizacji istotnych dla bezpieczeństwa;
    d) bezpiecznego wycofania produktu z użytku, w tym informacji o sposobie bezpiecznego usunięcia danych użytkownika.

ZAŁĄCZNIK III

PRODUKTY KRYTYCZNE Z ELEMENTAMI CYFROWYMI

Klasa I

1. Oprogramowanie systemów zarządzania tożsamością oraz oprogramowanie do zarządzania uprzywilejowanym dostępem.
2. Samodzielne i wbudowane przeglądarki.
3. Menedżer haseł.
4. Oprogramowanie, które wyszukuje, usuwa lub poddaje kwarantannie złośliwe oprogramowanie.
5. Produkty z elementami cyfrowymi z funkcją wirtualnej sieci prywatnej (VPN).
6. Systemy zarządzania siecią.
7. Narzędzia zarządzania konfiguracją sieci.
8. Systemy monitorowania ruchu w sieci.
9. Zarządzanie zasobami sieciowymi.
10. Systemy zarządzania informacjami i zdarzeniami zabezpieczeń (SIEM).
11. Zarządzanie aktualizacjami/poprawkami, w tym menedżer uruchamiania systemu.
12. Systemy zarządzania konfiguracją aplikacji.
13. Oprogramowanie do dostępu zdalnego/udostępniania.
14. Oprogramowanie do zarządzania urządzeniami mobilnymi.
15. Fizyczne interfejsy sieciowe.
16. Systemy operacyjne nieujęte w klasie II.
17. Zapory sieciowe, systemy wykrywania włamań lub zapobiegania włamaniom nieujęte w klasie II.
18. Routery, modemy przeznaczone do podłączenia do internetu oraz przełączniki nieujęte w klasie II.
19. Mikroprocesory nieujęte w klasie II.
20. Mikrokontrolery.
21. Specjalizowane układy scalone (ASIC) i bezpośrednio programowalne macierze bramek (FPGA) przeznaczone do użytku przez podmioty niezbędne takie jak podmioty, o których mowa w [załączniku I do dyrektywy XXX/XXXX (NIS 2)].
22. Systemy sterowania i automatyki przemysłowej (IACS) nieujęte w klasie II, takie jak programowalne sterowniki logiczne (PLC), rozproszone systemy sterowania (DCS), komputerowe sterowniki numeryczne (CNC) dla obrabiarek oraz systemy kontroli i gromadzenia danych (SCADA).
23. Przemysłowy internet rzeczy nieujęty w klasie II.

Klasa II

1. Systemy operacyjne do serwerów, komputerów stacjonarnych i urządzeń mobilnych.
2. Hiperwizory i systemy środowiska uruchomieniowego, które wspomagają zwirtualizowane wykonanie systemów operacyjnych i podobnych środowisk.
3. Infrastruktura klucza publicznego i wystawcy certyfikatów cyfrowych.
4. Zapory sieciowe, systemy wykrywania włamań lub zapobiegania włamaniom przeznaczone do zastosowania przemysłowego.
5. Mikroprocesory do zastosowań ogólnych.
6. Mikroprocesory przeznaczone do integracji z programowalnymi sterownikami logicznymi i zabezpieczeniami.
7. Routery, modemy przeznaczone do podłączenia do internetu oraz przełączniki przeznaczone do zastosowania przemysłowego.
8. Zabezpieczenia.
9. Sprzętowe moduły bezpieczeństwa (HSM).
10. Bezpieczne procesory kryptograficzne.
11. Karty inteligentne, czytniki kart inteligentnych i tokeny.
12. Systemy sterowania i automatyki przemysłowej (IACS) przeznaczone do użytku przez podmioty niezbędne takie jak podmioty, o których mowa w [załączniku I do dyrektywy XXX/XXXX (NIS 2)], takie jak programowalne sterowniki logiczne (PLC), rozproszone systemy sterowania (DCS), komputerowe sterowniki numeryczne (CNC) dla obrabiarek oraz systemy kontroli i gromadzenia danych (SCADA).
13. Urządzenia przemysłowego internetu rzeczy przeznaczone do użytku przez podmioty niezbędne takie jak podmioty, o których mowa w [załączniku I do dyrektywy XXX/XXXX (NIS 2)].
14. Komponenty czujników i aktuatorów robotów oraz sterowniki robotów.
15. Inteligentne liczniki.

ZAŁĄCZNIK IV

DEKLARACJA ZGODNOŚCI UE

W deklaracji zgodności UE, o której mowa w art. 20, należy zamieścić wszystkie następujące informacje:

1. nazwę i rodzaj oraz wszelkie dodatkowe informacje umożliwiające jednoznaczną identyfikację produktu z elementami cyfrowymi;
2. imię i nazwisko lub nazwę i adres producenta lub jego upoważnionego przedstawiciela;
3. oświadczenie, że deklarację zgodności UE wydano na wyłączną odpowiedzialność dostawcy;
4. przedmiot deklaracji (identyfikator produktu zapewniający możliwość jego śledzenia. W stosownych przypadkach może zawierać zdjęcie);
5. oświadczenie, że opisany powyżej przedmiot deklaracji jest zgodny z odnośnymi wymogami unijnego prawodawstwa harmonizacyjnego;
6. odniesienia do wszelkich zastosowanych odpowiednich norm zharmonizowanych lub wszelkich innych wspólnych specyfikacji, lub certyfikacji cyberbezpieczeństwa, z którymi deklaruje się zgodność;
7. w stosownych przypadkach nazwę i numer jednostki notyfikowanej, opis przeprowadzonej procedury oceny zgodności oraz dane identyfikacyjne wydanego certyfikatu;
8. informacje dodatkowe:

Podpisano w imieniu: ……

(miejsce i data wydania):

(imię i nazwisko, stanowisko) (podpis):

ZAŁĄCZNIK V

ZAWARTOŚĆ DOKUMENTACJI TECHNICZNEJ

Dokumentacja techniczna, o której mowa w art. 23, musi zawierać co najmniej następujące informacje, w zależności od tego, która z nich ma zastosowanie do odpowiedniego produktu z elementami cyfrowymi:

1. ogólny opis produktu z elementami cyfrowymi, w tym:
   a) jego przeznaczenie;
   b) wersje oprogramowania mające wpływ na zgodność z zasadniczymi wymogami;
   c) w przypadku gdy produkt z elementami cyfrowymi jest sprzętem, zdjęcia lub ilustracje przedstawiające cechy zewnętrzne, oznakowanie i układ wewnętrzny;
   d) informacje i instrukcje dla użytkowników zgodnie z treścią załącznika II;
2. opis projektowania, opracowywania i produkcji produktu oraz procedur postępowania w przypadku wykrycia podatności, w tym:
   a) kompletne informacje na temat projektowania i opracowywania produktu z elementami cyfrowymi, w tym, w stosownych przypadkach, rysunki i schematy lub opis architektury systemu wyjaśniający, w jaki sposób elementy oprogramowania współgrają ze sobą lub wzajemnie się uzupełniają oraz włączają się w ogólne przetwarzanie;
   b) kompletne informacje i specyfikacje wprowadzonych przez producenta procedur postępowania w przypadku wykrycia podatności, w tym zestawienie podstawowych materiałów do produkcji oprogramowania, politykę skoordynowanego ujawniania podatności, poświadczenie przedstawienia adresu do kontaktu do celów zgłaszania podatności oraz opis rozwiązań technicznych wybranych na potrzeby bezpiecznej dystrybucji aktualizacji;
   c) kompletne informacje i specyfikacje dotyczące procesów produkcji i monitorowania produktu z elementami cyfrowymi oraz walidacji tych procesów;
3. ocenę ryzyka w cyberprzestrzeni, na wypadek którego zaprojektowano, opracowano, wyprodukowano, dostarczono i utrzymywano produkt z elementami cyfrowymi, jak określono w art. 10 niniejszego rozporządzenia;
4. wykaz norm zharmonizowanych stosowanych w całości lub w części, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, wspólne specyfikacje określone w art. 19 niniejszego rozporządzenia lub programy certyfikacji cyberbezpieczeństwa przewidziane w rozporządzeniu (UE) 2019/881 zgodnie z art. 18 ust. 3 oraz – jeżeli nie zastosowano takich norm zharmonizowanych, wspólnych specyfikacji lub systemów certyfikacji cyberbezpieczeństwa – opisy rozwiązań przyjętych w celu spełnienia zasadniczych wymogów określonych w sekcjach 1 i 2 załącznika I, w tym wykaz innych odpowiednich zastosowanych specyfikacji technicznych. W przypadku częściowego zastosowania norm zharmonizowanych, wspólnych specyfikacji lub certyfikacji

cyberbezpieczeństwa w dokumentacji technicznej należy określić, które części zostały zastosowane;

5. sprawozdania z prób przeprowadzonych w celu weryfikacji zgodności produktu oraz procedur postępowania w przypadku wykrycia podatności z mającymi zastosowanie zasadniczymi wymogami określonymi w sekcjach 1 i 2 załącznika I;

6. kopię deklaracji zgodności UE;

7. w stosownych przypadkach zestawienie podstawowych materiałów do produkcji oprogramowania określone w art. 3 pkt 36, na uzasadniony wniosek organu nadzoru rynku, pod warunkiem że jest to niezbędne, aby organ ten mógł sprawdzić zgodność z zasadniczymi wymogami określonymi w załączniku I.

ZAŁĄCZNIK VI

PROCEDURY OCENY ZGODNOŚCI

Procedura oceny zgodności opierająca się na kontroli wewnętrznej (zgodnie z modułem A)

1. Kontrola wewnętrzna jest procedurą oceny zgodności, w ramach której producent wypełnia obowiązki określone w pkt 2, 3 i 4 oraz zapewnia i deklaruje, na swoją wyłączną odpowiedzialność, że produkt z elementami cyfrowymi spełnia wszystkie zasadnicze wymogi określone w sekcji 1 załącznika I, a producent spełnia zasadnicze wymogi określone w sekcji 2 załącznika I.

2. Producent ma obowiązek sporządzenia dokumentacji technicznej określonej w załączniku V.

3. Projektowanie, opracowywanie, produkcja i postępowanie w przypadku wykrycia podatności w odniesieniu do produktów z elementami cyfrowymi

   Producent ma obowiązek zastosowania wszelkich niezbędnych środków, aby projektowanie, opracowywanie, produkcja i procedury postępowania w przypadku wykrycia podatności, a także prowadzony przez niego monitoring zapewniały zgodność produkowanych lub opracowywanych produktów z elementami cyfrowymi i wprowadzonych przez producenta procedur z zasadniczymi wymogami określonymi w sekcjach 1 i 2 załącznika I.

4. Oznakowanie zgodności i deklaracja zgodności

4.1. Producent ma obowiązek umieszczenia oznakowania CE na każdym produkcie z elementami cyfrowymi spełniającym mające zastosowanie wymogi niniejszego rozporządzenia.

4.2. Producent ma obowiązek sporządzenia pisemnej deklaracji zgodności UE dla każdego produktu z elementami cyfrowymi zgodnie z art. 20 i przechowywania jej wraz z dokumentacją techniczną do dyspozycji organów krajowych przez okres 10 lat po wprowadzeniu do obrotu danego produktu z elementami cyfrowymi. W deklaracji zgodności UE należy wskazać produkt z elementami cyfrowymi, dla którego ją sporządzono. Kopię deklaracji zgodności UE należy udostępnić właściwym organom na żądanie.

5. Upoważnieni przedstawiciele

   Obowiązki producenta określone w pkt 4 mogą być w jego imieniu i na jego odpowiedzialność wypełniane przez jego upoważnionego przedstawiciela, pod warunkiem że zostały one wyszczególnione w upoważnieniu.

Badanie typu UE (zgodnie z modułem B)

1. Badanie typu UE jest elementem procedury oceny zgodności, w ramach której jednostka notyfikowana bada projektowanie i opracowywanie techniczne produktu oraz wprowadzone przez producenta procedury postępowania w przypadku wykrycia podatności, a także poświadcza, że produkt z elementami cyfrowymi spełnia

zasadnicze wymogi określone w sekcji 1 załącznika I oraz że producent spełnia zasadnicze wymogi określone w sekcji 2 załącznika I.

– Badanie typu UE polega na ocenie adekwatności projektowania i opracowywania technicznego produktu przez zbadanie dokumentacji technicznej i dowodów potwierdzających, o których mowa w pkt 3, oraz ocenę próbek co najmniej jednej z istotnych części produktu (połączenia typu produkcji i typu projektu).

2. Producent składa wniosek o badanie typu UE w jednej wybranej przez siebie jednostce notyfikowanej.

Wniosek taki musi zawierać:

– imię i nazwisko lub nazwę i adres producenta oraz, w przypadku wniosku składanego przez upoważnionego przedstawiciela, dodatkowo jego imię i nazwisko lub nazwę i adres;

– pisemną deklarację, że tego samego wniosku nie złożono w żadnej innej jednostce notyfikowanej;

– dokumentację techniczną, która musi umożliwiać przeprowadzenie oceny zgodności produktu z mającymi zastosowanie zasadniczymi wymogami określonymi w sekcji 1 załącznika I oraz oceny wprowadzonych przez producenta procedur postępowania w przypadku wykrycia podatności określonych w sekcji 2 załącznika I i która zawiera odpowiednią analizę i ocenę ryzyka. W dokumentacji technicznej należy określić mające zastosowanie wymogi i ująć, w stopniu właściwym dla oceny, projektowanie, produkcję i działanie produktu. W stosownych przypadkach dokumentacja techniczna musi zawierać co najmniej elementy określone w załączniku V;

– dowody potwierdzające adekwatność projektowania technicznego i rozwiązań dotyczących opracowywania oraz procedur postępowania w przypadku wykrycia podatności. W dowodach tych należy wymienić wszelkie wykorzystane dokumenty, w szczególności jeżeli nie zastosowano w pełni odpowiednich norm zharmonizowanych lub specyfikacji technicznych. W razie potrzeby dowody potwierdzające muszą obejmować wyniki testów przeprowadzonych przez odpowiednie laboratorium producenta lub przez inne laboratorium badawcze w jego imieniu i na jego odpowiedzialność.

3. Jednostka notyfikowana ma obowiązek:

3.1. badania dokumentacji technicznej i dowodów potwierdzających, aby ocenić adekwatność projektowania i opracowywania technicznego produktu w odniesieniu do zasadniczych wymogów określonych w sekcji 1 załącznika I oraz wprowadzonych przez producenta procedur postępowania w przypadku wykrycia podatności w odniesieniu do zasadniczych wymogów określonych w sekcji 2 załącznika I;

3.2. sprawdzania, czy egzemplarz lub egzemplarze opracowano lub wyprodukowano zgodnie z dokumentacją techniczną, i wskazywania elementów, które zostały zaprojektowane i opracowane zgodnie z mającymi zastosowanie przepisami odpowiednich norm zharmonizowanych lub specyfikacji technicznych, jak również tych elementów, które zostały zaprojektowane i opracowane bez stosowania odpowiednich przepisów tych norm;

3.3. przeprowadzania odpowiednich badań i testów lub zlecania ich przeprowadzenia, aby – w przypadku gdy producent zdecydował się na zastosowanie rozwiązań określonych w odpowiednich normach zharmonizowanych lub specyfikacjach technicznych odnoszących się do wymogów przewidzianych w załączniku I – sprawdzić, czy zastosowano je prawidłowo;

3.4. przeprowadzania odpowiednich badań i testów lub zlecania ich przeprowadzenia, aby – w przypadku gdy nie zastosowano rozwiązań określonych w odpowiednich normach zharmonizowanych lub specyfikacjach technicznych odnoszących się do wymogów przedstawionych w załączniku I – sprawdzić, czy rozwiązania przyjęte przez producenta spełniają odnośne zasadnicze wymogi;

3.5. uzgadniania z producentem miejsca, w którym zostaną przeprowadzone badania i testy.

4. Jednostka notyfikowana musi sporządzić sprawozdanie z oceny, w którym odnotowuje działania podjęte zgodnie z pkt 4 i ich rezultaty. Bez uszczerbku dla swoich obowiązków wobec organów notyfikujących jednostka notyfikowana udostępnia treść takiego sprawozdania, w całości lub w części, wyłącznie za zgodą producenta.

5. W sytuacji gdy typ oraz procedury postępowania w przypadku wykrycia podatności spełniają zasadnicze wymogi określone w załączniku I, jednostka notyfikowana wydaje producentowi certyfikat badania typu UE. Certyfikat musi zawierać imię i nazwisko lub nazwę i adres producenta, wnioski z badań, warunki (o ile występują) jego ważności oraz dane niezbędne do identyfikacji zatwierdzonego typu i procedur postępowania w przypadku wykrycia podatności. Do certyfikatu można dołączyć załącznik lub załączniki.

   Certyfikat i jego załączniki muszą zawierać wszystkie istotne informacje umożliwiające ocenę zgodności wyprodukowanych lub opracowanych produktów w odniesieniu do badanego typu i procedur postępowania w przypadku wykrycia podatności oraz kontrolę w trakcie eksploatacji.

   Jeżeli typ oraz procedury postępowania w przypadku wykrycia podatności nie spełniają mających zastosowanie zasadniczych wymogów określonych w załączniku I, jednostka notyfikowana odmawia wydania certyfikatu badania typu UE oraz informuje o tym wnioskodawcę, przedstawiając szczegółowe uzasadnienie odmowy.

6. Jednostka notyfikowana musi śledzić wszelkie zmiany w powszechnie uznanym stanie wiedzy technicznej wskazujące, że zatwierdzony typ oraz zatwierdzone procedury postępowania w przypadku wykrycia podatności mogą nie spełniać już mających zastosowanie zasadniczych wymogów określonych w załączniku I do niniejszego rozporządzenia, oraz musi ustalić, czy zmiany takie wymagają dalszego badania. Jeżeli ma to miejsce, jednostka notyfikowana musi poinformować o tym producenta.

   Producent ma obowiązek informowania jednostki notyfikowanej, która przechowuje dokumentację techniczną dotyczącą certyfikatu badania typu UE, o wszystkich modyfikacjach zatwierdzonego typu i zatwierdzonych procedur postępowania w przypadku wykrycia podatności mogących wpływać na zgodność z zasadniczymi wymogami określonymi w załączniku I lub warunkami ważności certyfikatu. Takie modyfikacje wymagają dodatkowego zatwierdzenia w formie dodatku do pierwotnego certyfikatu badania typu UE.

7. Każda jednostka notyfikowana musi poinformować właściwy organ notyfikujący o certyfikatach badania typu UE lub wszelkich dodatkach do nich, które wydała lub cofnęła, oraz, okresowo lub na żądanie, udostępniać właściwemu organowi notyfikującemu wykaz tych certyfikatów lub wszelkich dodatków do nich, których wydania odmówiła, które zawiesiła lub objęła innymi ograniczeniami.

   Każda jednostka notyfikowana musi poinformować pozostałe jednostki notyfikowane o certyfikatach badania typu UE lub wszelkich dodatkach do nich, których wydania odmówiła, które cofnęła, zawiesiła lub objęła innymi ograniczeniami oraz, na żądanie, o certyfikatach lub wszelkich dodatkach do nich, które wydała.

   Komisja, państwa członkowskie i pozostałe jednostki notyfikowane mogą otrzymać na żądanie kopie certyfikatów badania typu UE lub dodatków do nich. Komisja i państwa członkowskie mogą otrzymać na żądanie kopię dokumentacji technicznej oraz wyniki badań przeprowadzonych przez jednostkę notyfikowaną. Jednostka notyfikowana ma obowiązek przechowywania kopii certyfikatu badania typu UE, załączników i dodatków do niego, a także dokumentów technicznych, w tym dokumentacji przedłożonej przez producenta, do czasu wygaśnięcia ważności tego certyfikatu.

8. Producent ma obowiązek przechowywania kopii certyfikatu badania typu UE, załączników i dodatków do niego wraz z dokumentacją techniczną do dyspozycji organów krajowych przez okres 10 lat po wprowadzeniu produktu do obrotu.

9. Upoważniony przedstawiciel producenta może złożyć wniosek, o którym mowa w pkt 3, oraz wypełniać obowiązki określone w pkt 7 i 9, pod warunkiem że zostały one wyszczególnione w upoważnieniu.

Zgodność z typem w oparciu o wewnętrzną kontrolę produkcji (zgodnie z modułem C)

1. Zgodność z typem w oparciu o wewnętrzną kontrolę produkcji stanowi część procedury oceny zgodności, w ramach której producent wypełnia obowiązki określone w pkt 2 i 3 oraz zapewnia i deklaruje, że dane produkty są zgodne z typem opisanym w certyfikacie badania typu UE i spełniają zasadnicze wymogi przewidziane sekcji 1 załącznika I.

2. Produkcja

2.1. Producent ma obowiązek zastosowania wszelkich niezbędnych środków, aby proces produkcji i jego monitorowanie zapewniały zgodność wyprodukowanych produktów z zatwierdzonym typem opisanym w certyfikacie badania typu UE i z zasadniczymi wymogami przewidzianymi w sekcji 1 załącznika I.

3. Oznakowanie zgodności i deklaracja zgodności

3.1. Producent ma obowiązek umieszczenia oznakowania CE na każdym egzemplarzu produktu zgodnym z typem opisanym w certyfikacie badania typu UE i spełniającym mające zastosowanie wymogi instrumentu legislacyjnego.

3.2. Producent ma obowiązek sporządzenia pisemnej deklaracji zgodności dla modelu produktu i przechowywania jej do dyspozycji organów krajowych przez okres 10 lat po wprowadzeniu produktu do obrotu. W deklaracji zgodności należy wskazać produkt, dla którego została ona sporządzona. Kopię deklaracji zgodności należy udostępnić na żądanie właściwych organów.

4. Upoważniony przedstawiciel

Obowiązki producenta określone w pkt 3 mogą być wypełniane w jego imieniu i na jego odpowiedzialność przez upoważnionego przedstawiciela, pod warunkiem że zostały one wyszczególnione w upoważnieniu.

Zgodność oparta na pełnym zapewnieniu jakości (zgodnie z modułem H)

1. Zgodność oparta na pełnym zapewnieniu jakości jest procedurą oceny zgodności, według której producent wypełnia obowiązki określone w pkt 2 i 5 oraz zapewnia i deklaruje, na swoją wyłączną odpowiedzialność, że dane produkty (lub kategorie produktów) spełniają zasadnicze wymogi określone w sekcji 1 załącznika I, a wprowadzone przez producenta procedury postępowania w przypadku wykrycia podatności spełniają zasadnicze wymogi określone w sekcji 2 załącznika I.

2. Projektowanie, opracowywanie, produkcja i postępowanie w przypadku wykrycia podatności w odniesieniu do produktów z elementami cyfrowymi

Producent ma obowiązek posiadania zatwierdzonego systemu jakości określonego w pkt 3 w odniesieniu do projektowania, opracowywania i produkcji przedmiotowych produktów oraz w odniesieniu do postępowania w przypadku wykrycia podatności oraz utrzymania wydajności tychże produktów przez cały cykl ich życia, a także podlega nadzorowi zgodnie z pkt 4.

3. System jakości

3.1. Producent ma obowiązek złożenia w wybranej przez siebie jednostce notyfikowanej wniosku o ocenę jego systemu jakości dla danych produktów.

Wniosek taki musi zawierać:

– imię i nazwisko lub nazwę i adres producenta oraz, w przypadku wniosku składanego przez upoważnionego przedstawiciela, dodatkowo jego imię i nazwisko lub nazwę i adres;

– dokumentację techniczną dla jednego modelu każdej kategorii produktów, które mają być produkowane lub opracowywane. W stosownych przypadkach dokumentacja techniczna musi zawierać co najmniej elementy określone w załączniku V;

– dokumentację dotyczącą systemu jakości oraz

– pisemną deklarację, że tego samego wniosku nie złożono w żadnej innej jednostce notyfikowanej.

3.2. System jakości musi zapewniać zgodność produktów z zasadniczymi wymogami określonymi w sekcji 1 załącznika I oraz zgodność wprowadzonych przez producenta procedur postępowania w przypadku wykrycia podatności z wymogami określonymi w sekcji 2 załącznika I.

Wszystkie elementy, wymogi i środki przyjęte przez producenta muszą być w systematyczny i uporządkowany sposób udokumentowane w formie pisemnych zaleceń, procedur i instrukcji. Dokumentacja systemu jakości musi umożliwiać spójną interpretację programów, planów, ksiąg i zapisów dotyczących jakości.

Dokumentacja ta musi zawierać w szczególności stosowny opis:

– celów jakości i struktury organizacyjnej, obowiązków oraz uprawnień kierownictwa w odniesieniu do projektowania, opracowywania, jakości produktu i postępowania w przypadku wykrycia podatności;

– specyfikacji technicznych projektowania i opracowywania, w tym norm, które będą stosowane, oraz – w przypadku gdy nie będą w pełni stosowane odnośne normy zharmonizowane lub specyfikacje techniczne – środków, które zostaną wprowadzone w celu zapewnienia spełnienia zasadniczych wymogów określonych w sekcji 1 załącznika I mających zastosowanie do produktów;

– specyfikacji procedur, w tym norm, które będą stosowane, oraz – w przypadku gdy nie będą w pełni stosowane odnośne normy zharmonizowane lub specyfikacje techniczne – środków, które zostaną wprowadzone w celu zapewnienia spełnienia zasadniczych wymogów określonych w sekcji 2 załącznika I mających zastosowanie do producenta;

– kontroli projektowania i opracowywania oraz technik weryfikacji projektowania i opracowywania, procesów i systematycznych działań, które będą podejmowane podczas projektowania i opracowywania produktów należących do danej kategorii produktów;

– odpowiednich technik produkcji, kontroli jakości i zapewnienia jakości, procesów i systematycznych działań, które będą podejmowane;

– badań i testów, które będą wykonywane przed rozpoczęciem, w trakcie i po zakończeniu produkcji oraz ich częstotliwości;

– zapisów dotyczących jakości, takich jak sprawozdania z kontroli i dane z badań, dane dotyczące wzorcowania, sprawozdania dotyczące kwalifikacji odpowiedniego personelu itp.;

– środków monitorowania osiągania wymaganej jakości projektowania i produktu oraz skutecznego działania systemu jakości.

3.3. Jednostka notyfikowana ma obowiązek oceny systemu jakości w celu stwierdzenia, czy spełnia on wymogi, o których mowa w pkt 3.2.

Zakłada ona zgodność z tymi wymogami w odniesieniu do elementów systemu jakości zgodnych z odpowiednimi specyfikacjami normy krajowej wdrażającej odnośną normę zharmonizowaną lub specyfikację techniczną.

Oprócz doświadczenia w zakresie systemów zarządzania jakością co najmniej jeden członek zespołu audytowego musi mieć doświadczenie z zakresu oceny w dziedzinie danego produktu i danej technologii, a także znać mające zastosowanie wymogi niniejszego rozporządzenia. Audyt musi obejmować wizytę oceniającą w zakładzie producenta, jeżeli taki zakład istnieje. Zespół audytowy ma za zadanie dokonać przeglądu dokumentacji technicznej, o której mowa w pkt 3.1 tiret drugie, w celu weryfikacji zdolności producenta do identyfikowania mających zastosowanie wymogów niniejszego rozporządzenia oraz do przeprowadzenia koniecznych badań w celu zapewnienia zgodności produktu z tymi wymogami.

O decyzji należy powiadomić producenta lub jego upoważnionego przedstawiciela.

Powiadomienie takie musi zawierać wnioski z audytu oraz uzasadnioną decyzję dotyczącą dokonanej oceny.

3.4. Producent podejmuje się wypełnienia zobowiązań wynikających z zatwierdzonego systemu jakości oraz utrzymania go w taki sposób, aby pozostawał odpowiedni oraz wydajny.

3.5. Producent musi na bieżąco informować jednostkę notyfikowaną, która zatwierdziła system jakości, o wszelkich zamierzonych modyfikacjach systemu jakości.

Jednostka notyfikowana musi ocenić proponowane zmiany oraz zdecydować, czy zmodyfikowany system jakości nadal będzie spełniał wymogi, o których mowa w pkt 3.2, lub czy konieczna jest ponowna jego ocena.

Musi powiadomić producenta o swojej decyzji. Powiadomienie takie musi zawierać wnioski z badania oraz uzasadnioną decyzję dotyczącą dokonanej oceny.

4. Nadzór, za który odpowiedzialna jest jednostka notyfikowana

4.1. Celem nadzoru jest sprawdzenie, czy producent należycie wypełnia obowiązki wynikające z zatwierdzonego systemu jakości.

4.2. Do celów oceny producent ma obowiązek umożliwienia jednostce notyfikowanej dostępu do miejsc projektowania, opracowywania, produkcji, kontroli, badań i magazynowania oraz przedstawienia wszelkich niezbędnych informacji, a w szczególności:

– dokumentacji systemu jakości;

– zapisów dotyczących jakości przewidzianych w projektowej części systemu jakości, takich jak wyniki analiz, obliczeń, badań itp.;

– zapisów dotyczących jakości przewidzianych w produkcyjnej części systemu jakości, takich jak sprawozdania z kontroli i dane z badań, dane dotyczące wzorcowania, sprawozdania dotyczące kwalifikacji odpowiedniego personelu itp.

4.3. Jednostka notyfikowana ma obowiązek przeprowadzania okresowych audytów mających na celu sprawdzenie, czy producent utrzymuje i stosuje system jakości, oraz przekazywania producentowi sprawozdania z audytu.

5. Oznakowanie zgodności i deklaracja zgodności

5.1. Producent ma obowiązek umieszczenia oznakowania CE oraz, na odpowiedzialność jednostki notyfikowanej, o której mowa w pkt 3.1, jej numeru identyfikacyjnego na każdym egzemplarzu produktu spełniającym wymogi określone w sekcji 1 załącznika I do niniejszego rozporządzenia.

5.2. Producent ma obowiązek sporządzenia pisemnej deklaracji zgodności dla każdego modelu produktu i przechowywania jej do dyspozycji organów krajowych przez okres 10 lat po wprowadzeniu produktu do obrotu. W deklaracji zgodności należy wskazać produkt, dla którego została ona sporządzona.

Kopię deklaracji zgodności należy udostępnić na żądanie właściwych organów.

6. Producent ma obowiązek przechowywania przez okres co najmniej 10 lat od wprowadzenia produktu do obrotu następujących dokumentów, które są udostępniane organom krajowym:

– dokumentacji technicznej, o której mowa w pkt 3.1;

– dokumentacji dotyczącej systemu jakości, o której mowa w pkt 3.1;

– zatwierdzonej zmiany, o której mowa w pkt 3.5,

– decyzji i sprawozdań jednostki notyfikowanej, o których mowa w pkt 3.5, 4.3 i 4.4.

7. Każda jednostka notyfikowana ma obowiązek informowania odnośnych organów notyfikujących o wydanych lub cofniętych zatwierdzeniach systemów jakości oraz, okresowo lub na żądanie, udostępniania odnośnym organom notyfikującym wykazu zatwierdzeń systemów jakości, których wydania odmówiono, które zawieszono lub poddano innym ograniczeniom.

Każda jednostka notyfikowana musi informować pozostałe jednostki notyfikowane o zatwierdzeniach systemów jakości, których wydania odmówiła, które cofnęła lub zawiesiła oraz, na żądanie, o zatwierdzeniach systemów jakości, które wydała.

8. Upoważniony przedstawiciel

Obowiązki producenta określone w pkt 3.1, 3.5, 5 i 6 może w jego imieniu i na jego odpowiedzialność wypełniać jego upoważniony przedstawiciel, pod warunkiem że zostały one wyszczególnione w upoważnieniu.