

				Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII11				Tytuł dokumentu: Polityka prawidłowości i jakości PII							
Wersja: 1.0		Data wejścia w życie: 01.01.2025		Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne

Historia zmian				
Numer zmiany	Data zmiany	Zmiany	Przegląd wykonał	Właściciel procesu

Zatwierdzenia			
Imię i nazwisko	Stanowisko	Data	Podpis

Nota prawna (prawa autorskie i ograniczenia użytkowania)

(C) 2025 Clarysec LLC. All rights reserved.

Niniejszy dokument stanowi własność intelektualną spółki Clarysec LLC. Żadna część tego dokumentu nie może być kopiowana, ponownie wykorzystywana, rozpowszechniana ani modyfikowana do celów komercyjnych lub wdrożeniowych bez uprzedniej wyraźnej pisemnej zgody.

Nieuprawnione użycie jest surowo zabronione i może skutkować podjęciem kroków prawnych.

W sprawach licencjonowania prosimy o kontakt: info@clarysec.com

Dostosowanie do norm i regulacji

Norma / regulacja	Klauzula / środek kontrolny / artykuł	Applicability	Coverage Type	Komentarz
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Udokumentowane dowody prawidłowości i kontrola operacyjna
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorowanie, niezgodność i działanie korygujące
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Rejestry przetwarzania administratora
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.7	Controller	Primary	Obowiązki dotyczące prawidłowości i mechanizmy sprostowania
ISO/IEC 27701:2025	Annex A.1.3.8	Controller	Primary	Powiadomienie właściwych odbiorców o sprostowaniu
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Polecenia, wsparcie i rejestry podmiotu przetwarzającego
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Wsparcie podmiotu przetwarzającego w zakresie sprostowania
GDPR	Article 5(1)(d); Article 5(2)	Controller	Primary	Prawidłowość i rozliczalność
GDPR	Article 16	Controller	Primary	Sprostowanie
GDPR	Article 19	Controller	Primary	Powiadomienie odbiorcy
GDPR	Article 24	Controller	Supporting	Środki administratora
GDPR	Article 28	Both	Supporting	Pomoc podmiotu przetwarzającego i polecenia
GDPR	Article 30	Both	Supporting	Rejestry przetwarzania

ISO/IEC 29100:2020	Clause 5.7	Both	Primary	Zasada prawidłowości i jakości
ISO/IEC 29151:2022	Annex A.8	Both	Primary	Środki kontrolne dotyczące prawidłowości i jakości PII

1. Zakres

1.1 Niniejsza polityka określa wymagania dotyczące utrzymywania prawidłowości, kompletności, aktualności, adekwatności i relewantności PII przetwarzanych w zakresie PIMS.

1.2 Niniejsza polityka ma zastosowanie w kontekstach administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania. Obowiązki administratora są podstawowe. Obowiązki podmiotu przetwarzającego i podwykonawcy przetwarzania mają zastosowanie, gdy organizacja wspiera administratora w sprostowaniu, synchronizacji lub realizacji poleceń dotyczących prawidłowości.

1.3 Niniejsza polityka obejmuje:

1.3.1 odpowiedzialność za prawidłowość według czynności przetwarzania;

1.3.2 kontrole prawidłowości danych w punktach gromadzenia, importu, zmiany źródła i przeglądu;

1.3.3 przesłanki sprostowania i walidację;

1.3.4 przegląd nieaktualnych danych dla rekordów o istotnym wpływie;

1.3.5 synchronizację zatwierdzonych sprostowań w odpowiednich systemach i u dalszych stron;

1.3.6 wsparcie podmiotu przetwarzającego i podwykonawcy przetwarzania w zakresie sprostowania;

1.3.7 dowody w REG02, REG06, REG08 i REG12.

1.4 Niniejsza polityka nie ustanawia odrębnego programu jakości danych, rejestru jakości danych, funkcji nadzoru nad danymi podstawowymi, ram jakości danych analitycznych ani ram jakości danych treningowych AI.

1.5 Niniejsza polityka nie zastępuje:

1.5.1 PII03 w zakresie inwentarza przetwarzania, celów, podstawy prawnej i własności REG02;

1.5.2 PII06 w zakresie przyjmowania wniosków osób, których dane dotyczą, o realizację praw, weryfikacji tożsamości, ustawowej obsługi odpowiedzi i komunikacji zamykającej sprawę;

1.5.3 PII10 w zakresie wykonywania okresu przechowywania, usuwania, kasowania i utylizacji;

1.5.4 PII12 w zakresie zarządzania cyklem życia podmiotu przetwarzającego, podwykonawcy przetwarzania i strony trzeciej;

1.5.5 PII14 w zakresie bezpieczeństwa PII i kontroli dostępu;

1.5.6 PII18 w zakresie monitorowania, audytu, niezgodności, działań korygujących i zarządzania doskonaleniem w całym PIMS.

1.6 Na potrzeby niniejszej polityki rekord o istotnym wpływie oznacza rekord PII używany do przyznania, odmowy, zmiany lub istotnego wpływania na dostęp do usługi, umowy, sprawy pracowniczej, wyniku finansowego, wyniku związanego ze zdrowiem, decyzji o kwalifikowalności, decyzji dotyczącej tożsamości, decyzji dotyczącej ryzyka albo innej decyzji, w przypadku której nieprawidłowe PII mogłyby istotnie wpłynąć na osobę, której dane dotyczą.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby PII wykorzystywane przez organizację pozostawały prawidłowe i odpowiednie do celów przetwarzania zapisanych w PIMS, a także aby nieprawidłowe, niekompletne, nieaktualne lub kwestionowane PII były sprostowywane, synchronizowane albo eskalowane z wykorzystaniem kontrolowanych dowodów.

3. Cele

3.1 Celami niniejszej polityki są:

3.1.1 przypisanie odpowiedzialności za prawidłowość dla każdej odpowiedniej czynności przetwarzania;

- 3.1.2 zdefiniowanie prostych i testowalnych kontroli prawidłowości danych bez tworzenia odrębnego programu ładu danych;
- 3.1.3 ustanowienie jasnych przesłanek sprostowania, przeglądu nieaktualnych danych i synchronizacji;
- 3.1.4 wspieranie wniosków osób, których dane dotyczą, o sprostowanie bez powielania procesu obsługi wniosków o realizację praw;
- 3.1.5 wspieranie pomocy podmiotu przetwarzającego i podwykonawcy przetwarzania w zakresie sprostowania na podstawie udokumentowanych poleceń;
- 3.1.6 przechowywanie dowodów w REG02, REG06, REG08 i REG12;
- 3.1.7 eskalowanie powtarzających się, zaległych lub dotyczących istotnego wpływu problemów z prawidłowością za pośrednictwem procesu działań korygujących PIMS.

4. Postanowienia polityki

4.1 Odpowiedzialność za prawidłowość i wymagania dotyczące prawidłowości

- 4.1.1 [Controller] Process Owner / Business Owner MUSI zapisać właściciela prawidłowości, autorytatywne źródło, oznaczenie rekordu o istotnym wpływie oraz częstotliwość przeglądu prawidłowości dla każdej czynności przetwarzania w roli administratora w REG02 przed rozpoczęciem przetwarzania oraz w terminie 10 dni roboczych od istotnej zmiany przetwarzania.
- 4.1.2 [Joint Controller] Vendor / Procurement Owner MUSI zapisać w REG08 podział odpowiedzialności za prawidłowość między współadministratorami oraz powiązać go z właściwą czynnością przetwarzania w REG02 przed rozpoczęciem przetwarzania w roli współadministratorów.
- 4.1.3 [Processor] Vendor / Procurement Owner MUSI zapisać obowiązki wsparcia sprostowań wobec klienta oraz autoryzowany kanał poleceń w REG08 przed onboardingiem usługi podmiotu przetwarzającego oraz w terminie 10 dni roboczych od istotnej zmiany umowy.
- 4.1.4 [Both] Process Owner / Business Owner MUSI zdefiniować minimalne kontrole prawidłowości danych dla każdej kategorii PII wykorzystywanej w przypisanej czynności przetwarzania w REG02 przed rozpoczęciem przetwarzania, a następnie corocznie.
- 4.1.5 [Controller] Process Owner / Business Owner MUSI sklasyfikować rekordy o istotnym wpływie w REG02 przed rozpoczęciem przetwarzania w roli administratora, a następnie corocznie.
- 4.1.6 [Both] Privacy Lead / PIMS Manager MUSI kwartalnie przeglądać odpowiedzialność za prawidłowość, oznaczenia istotnego wpływu i cykl przeglądów w REG02 oraz zapisywać nierozwiązane luki w REG12 w terminie pięciu dni roboczych od zakończenia przeglądu.

4.2 Kontrole prawidłowości danych i przegląd nieaktualnych danych

- 4.2.1 [Controller] Process Owner / Business Owner MUSI zapisać wykonanie zdefiniowanej kontroli prawidłowości danych w REG02, zanim nowo zgromadzone PII zostaną wykorzystane do aktywnego przetwarzania w roli administratora.
- 4.2.2 [Controller] Process Owner / Business Owner MUSI zweryfikować wiarygodność PII zgromadzonych ze źródła innego niż osoba, której dane dotyczą, w REG02 przed pierwszym użyciem oraz przed każdą istotną zmianą źródła.
- 4.2.3 [Both] Process Owner / Business Owner MUSI przeglądać aktywne rekordy o istotnym wpływie w REG02 co najmniej corocznie oraz przed poleganiem na rekordzie o istotnym wpływie, którego termin przeglądu jest zaległy.

- 4.2.4 [Both] System Owner / Application Owner MUSI zidentyfikować wskaźniki nieaktualnych danych dla rekordów systemowych o istotnym wpływie w REG02 przed uruchomieniem produkcyjnym systemu oraz w terminie 30 dni od istotnej zmiany systemu.
- 4.2.5 [Both] Process Owner / Business Owner MUSI zapisać wewnętrzny problem z prawidłowością w REG12 w terminie pięciu dni roboczych, gdy kontrola prawidłowości danych wykryje nieprawidłowe, niekompletne, nieaktualne, niespójne lub niepoparte dowodami PII, które nie zostały zgłoszone jako wniosek osoby, której dane dotyczą, o sprostowanie.
- 4.2.6 [Controller] Privacy Lead / PIMS Manager MUSI powiązać każde żądanie sprostowania pochodzące od osoby, której dane dotyczą, w REG06 z właściwą czynnością przetwarzania w REG02 w terminie pięciu dni roboczych od przypisania do merytorycznego przeglądu prawidłowości.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Wyjątki

9.1 Wyjątki dotyczące prawidłowości

- 9.1.1 [Both] Process Owner / Business Owner MUSI wystąpić o wyjątek dotyczący prawidłowości w REG12 przed wykorzystaniem znanych niezwyfikowanych, nieaktualnych lub kwestionowanych PII poza zapisaną częstotliwością przeglądu.
- 9.1.2 [Both] Privacy Lead / PIMS Manager MUSI ocenić wpływ i mitygację każdego wyjątku dotyczącego prawidłowości w REG12 w terminie pięciu dni roboczych od wniosku.
- 9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUSI zapisać poradę w REG12 przed zatwierdzeniem wyjątku dotyczącego prawidłowości obejmującego rekordy o istotnym wpływie, kwestionowane sprostowanie lub wymóg prawny.
- 9.1.4 [All] Top Management MUSI zatwierdzić wyjątek dotyczący prawidłowości wpływający na rekordy o istotnym wpływie, nierozwiązane sprostowania, zakres certyfikacji lub obowiązki prawne w REG12 przed wejściem wyjątku w życie.
- 9.1.5 [Both] Privacy Lead / PIMS Manager MUSI ustalić datę wygaśnięcia nieprzekraczającą 90 dni w REG12 dla każdego zatwierzonego wyjątku dotyczącego prawidłowości przed zatwierdzeniem.
- 9.1.6 [Both] Privacy Lead / PIMS Manager MUSI zamknąć lub ponownie ocenić każdy wyjątek dotyczący prawidłowości w REG12 w terminie pięciu dni roboczych od wygaśnięcia.

10. Egzekwowanie postanowień

10.1 Egzekwowanie i obsługa niezgodności

- 10.1.1 [Both] Privacy Lead / PIMS Manager MUSI zapisać zaległy przegląd o istotnym wpływie, niesprostowane nieprawidłowe PII lub pominiętą synchronizację jako niezgodność w REG12 w terminie pięciu dni roboczych od identyfikacji.
- 10.1.2 [Both] System Owner / Application Owner MUSI uniemożliwić uruchomienie produkcyjnego systemu przetwarzającego PII o istotnym wpływie, gdy REG02 nie zawiera wymaganego właściciela prawidłowości, metody kontroli prawidłowości danych lub ścieżki sprostowania, oraz zapisać decyzję w REG12 przed uruchomieniem produkcyjnym.
- 10.1.3 [Controller] Process Owner / Business Owner MUSI zawiesić poleganie na znanych nieprawidłowych PII o istotnym wpływie przy istotnych decyzjach do czasu zapisania sprostowania, ograniczenia lub zatwierzonego wyjątku w REG06 lub REG12.
- 10.1.4 [Both] Vendor / Procurement Owner MUSI eskalować brak wsparcia zatwierzonego sprostowania przez podmiot przetwarzający, podwykonawcę przetwarzania lub odbiorcę w REG08 i REG12 w terminie pięciu dni roboczych po terminie wsparcia.

- 10.1.5 [All] Top Management MUSI wymagać działania korygującego w REG12 w terminie 10 dni roboczych w przypadku powtarzającej się lub długotrwałej nieskuteczności prawidłowości o istotnym wpływie.
- 10.1.6 [All] Internal Audit / Compliance Reviewer MUSI zweryfikować skuteczność działań korygujących dotyczących niezgodności w zakresie prawidłowości PII w REG12 podczas następnego zaplanowanego audytu PIMS albo w terminie 60 dni od zamknięcia, w zależności od tego, co nastąpi wcześniej.

11. Przegląd i utrzymanie

11.1 Przegląd polityki i środków kontrolnych prawidłowości

- 11.1.1 [All] Privacy Lead / PIMS Manager MUSI przeglądać niniejszą politykę w REG12 corocznie oraz w terminie 30 dni od istotnej zmiany prawnej, przetwarzania, systemu lub zakresu certyfikacji.
- 11.1.2 [Both] Process Owner / Business Owner MUSI przeglądać odpowiedzialność za prawidłowość, klasyfikację istotnego wpływu i cykl przeglądów w REG02 corocznie oraz w terminie 30 dni od istotnej zmiany przetwarzania.
- 11.1.3 [Both] System Owner / Application Owner MUSI przeglądać ścieżkę sprostowania i procedurę synchronizacji zapisane w REG02 corocznie oraz w terminie 30 dni od istotnej zmiany systemu.
- 11.1.4 [Both] Vendor / Procurement Owner MUSI przeglądać obowiązki wsparcia sprostowań przez podmiot przetwarzający, podwykonawcę przetwarzania, odbiorcę i stronę udostępniania danych w REG08 przed odnowieniem oraz w terminie 30 dni od istotnej zmiany relacji.
- 11.1.5 [Conditional] Data Protection Officer / Privacy Advisor MUSI przeglądać wpływ istotnych zmian polityki na prywatność w REG12 przed zatwierdzeniem.
- 11.1.6 [All] Top Management MUSI zatwierdzać istotne zmiany niniejszej polityki w REG12 przed publikacją.

12. Powiązane polityki

- 12.1 PII01 - Polityka systemu zarządzania informacjami o prywatności
- 12.2 PII02 - Polityka ról, odpowiedzialności i rozliczalności w zakresie prywatności
- 12.3 PII03 - Polityka inwentarza przetwarzania PII i podstawy prawnej
- 12.4 PII06 - Polityka zarządzania prawami osób, których dane dotyczą
- 12.5 PII08 - Polityka privacy by design i privacy by default
- 12.6 PII09 - Polityka gromadzenia, wykorzystywania, ujawniania i udostępniania PII
- 12.7 PII10 - Polityka okresu przechowywania, usuwania i utylizacji PII
- 12.8 PII12 - Polityka zarządzania prywatnością podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich
- 12.9 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu
- 12.10 PII17 - Polityka udokumentowanych informacji i zarządzania dowodami PIMS
- 12.11 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS

13. Normy i ramy odniesienia

- 13.1 Niniejsza polityka jest zmapowana do następujących norm i regulacji. Mapowanie wyjaśnia, w jaki sposób polityka wspiera przywołane wymagania, oraz wskazuje klauzule wewnętrzne, które je wdrażają lub wspierają.

13.2 ISO/IEC 27701:2025

- 13.2.1 **Clause 7.5; Clause 8.1** - Zmapowano do udokumentowanych wymagań dotyczących prawidłowości, dowodów REG02 i REG06, procesu sprostowania danych, procesu

- synchronizacji, odpowiedzialności wdrożeniowych i kontroli operacyjnych. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.3.1; 4.3.2; 4.3.4; 4.3.5; 4.4.1; 4.4.2; 5.1.2; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 7.1.5; 7.1.6; 7.1.7].
- 13.2.2 **Clause 9.1; Clause 10.2** - Zmapowano do monitorowania prawidłowości, metryk, zapisywania niezgodności, działań korygujących, eskalacji, próbkowania audytowego i weryfikacji skuteczności. Addressed by clauses [4.1.6; 4.2.5; 4.5.1; 4.5.2; 4.5.3; 4.5.5; 5.1.7; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].
- 13.2.3 **Annex A.1.2.9** - Zmapowano do rejestrów przetwarzania administratora, odpowiedzialności za prawidłowość, źródła, klasyfikacji istotnego wpływu, częstotliwości przeglądu i aktualizacji REG02. Addressed by clauses [4.1.1; 4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 5.1.4; 7.1.1; 7.1.3; 11.1.2].
- 13.2.4 **Annex A.1.3.2; Annex A.1.3.7** - Zmapowano do ustalania i realizacji obowiązków administratora w zakresie sprostowania, walidacji, zatwierdzania sprostowania, wdrażania sprostowania, obsługi sporów i dowodów zamknięcia. Addressed by clauses [4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.3.7; 7.1.5; 7.1.6; 7.1.7; 9.1.3; 10.1.3].
- 13.2.5 **Annex A.1.3.8** - Zmapowano do powiadamiania właściwych dalszych stron i śledzenia potwierdzeń zatwierdzonych sprostowań. Addressed by clauses [4.4.3; 4.4.7; 5.1.6; 7.1.4; 8.1.3; 10.1.4; 11.1.4].
- 13.2.6 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Zmapowano do dowodów umowy klienta z podmiotem przetwarzającym, obowiązków wsparcia sprostowań wobec klienta, autoryzowanych kanałów poleceń i rejestrów podmiotu przetwarzającego. Addressed by clauses [4.1.3; 4.4.4; 4.4.5; 5.1.6; 7.1.4; 10.1.4; 11.1.4].
- 13.2.7 **Annex A.2.3.2** - Zmapowano do środków podmiotu przetwarzającego służących wspieraniu obowiązków administratora w zakresie sprostowania na podstawie udokumentowanego polecenia. Addressed by clauses [4.1.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 5.1.5; 5.1.6; 7.1.4; 10.1.4].

13.3 **GDPR**

- 13.3.1 **Article 5(1)(d); Article 5(2)** - Zmapowano do odpowiedzialności za prawidłowość, kontroli, przeglądu nieaktualnych danych, sprostowania, synchronizacji, dowodów, monitorowania i rejestrów rozliczalności. Addressed by clauses [4.1.1; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.2; 4.3.4; 4.4.2; 4.5.1; 6.1.1; 8.1.1; 8.1.2; 10.1.1].
- 13.3.2 **Article 16** - Zmapowano do walidacji, zatwierdzania, wdrożenia i zamknięcia pozycji sprostowania zapisanych w REG06 i REG02. Addressed by clauses [4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 7.1.5; 7.1.6; 7.1.7].
- 13.3.3 **Article 19** - Zmapowano do powiadamiania odbiorcy, podmiotu przetwarzającego i dalszych stron o sprostowaniu oraz śledzenia potwierdzeń. Addressed by clauses [4.4.3; 4.4.7; 5.1.6; 7.1.4; 8.1.3; 10.1.4; 11.1.4].
- 13.3.4 **Article 24** - Zmapowano do środków administratora, odpowiedzialności, przeglądu zarządzania, wyjątków, eskalacji i działań korygujących dotyczących środków kontrolnych prawidłowości. Addressed by clauses [4.1.1; 4.1.5; 4.5.1; 4.5.5; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].
- 13.3.5 **Article 28** - Zmapowano do wsparcia sprostowań przez podmiot przetwarzający i podwykonawcę przetwarzania, udokumentowanych poleceń, wdrożenia autoryzowanego przez klienta oraz eskalacji braku wsparcia. Addressed by clauses [4.1.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 5.1.6; 7.1.4; 10.1.4; 11.1.4].
- 13.3.6 **Article 30** - Zmapowano do rejestrów przetwarzania wykorzystywanych do wykazania odpowiedzialności za prawidłowość, źródeł, klasyfikacji istotnego wpływu, powiązań

systemowych i aktualizacji czynności przetwarzania. Addressed by clauses [4.1.1; 4.1.4; 4.1.5; 4.2.2; 4.2.3; 4.4.1; 4.5.4; 7.1.1; 7.1.2; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.7** - Zmapowano do oczekiwań dotyczących prawidłowości i jakości PII, obejmujących PII prawidłowe, kompletne, aktualne, adekwatne i relewantne, w tym wiarygodność źródeł, walidację sprostowania i okresowe kontrole. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.2; 4.3.4; 4.3.5; 4.4.2; 8.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.8** - Zmapowano do środków kontrolnych dotyczących prawidłowości i jakości PII w zakresie procedur gromadzenia, wiarygodności źródeł, walidacji, okresowego przeglądu, sprostowania i mechanizmów aktualizacji o istotnym wpływie. Addressed by clauses [4.1.1; 4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.2; 4.3.4; 4.4.1; 4.4.2; 4.5.3; 7.1.2; 7.1.3; 11.1.3].