

		Въведете тук наименованието на регистрираното юридическо лице					
Номер на документа: PII23		Заглавие на документа: Политика за обработващ лични данни в облачна среда					
Версия: 1.0	Дата на влизане в сила: 01.01.2025	Собственик на документа:					
X	Политика		Стандарт	Процедура	Формуляр	Регистър	Друго

История на редакциите				
Номер на редакцията	Дата на редакцията	Промени	Прегледано от	Собственик на процеса

Одобрения			
Име	Длъжност	Дата	Подпис

Правна бележка (авторски права и ограничения за ползване)
 (C) 2025 Clarysec LLC. All rights reserved.

Настоящият документ е интелектуална собственост на Clarysec LLC. Никаква част от него не може да бъде копирана, използвана повторно, разпространявана или изменяна за търговски или внедрителски цели без изрично писмено разрешение.

Неупълномощеното използване е строго забранено и може да доведе до правни действия.

За лицензиране се свържете с: info@clarysec.com

Съгласуване със стандарти и регулации

Стандарт / регулация	Клауза / контрол / член	Приложимост	Вид покритие	Коментар
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	Роля в PIMS и приложимост на контролите
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Документирани доказателства за обработващ лични данни в облачна среда и оперативен контрол
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Мониторинг, несъответствие и коригиращо действие
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Споразумения с клиенти, нареждания, съдействие и записи
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Съдействие на клиенти във връзка със задължения към субекти на данни
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Контроли за временни файлове, връщане, прехвърляне, унищожаване и предаване
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Основание и местоположения за прехвърляне
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Записи за разкриване и обработване на искания за разкриване
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Разкриване на подизпълнители по обработване, ангажиране и уведомяване за промяна

ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25	Processor	Supporting	Доказателства за достъп, записи, резервни копия и журнализиране
GDPR	Article 28	Processor	Primary	Обработващ лични данни, подизпълнител по обработване, съдействие, одит, изтриване и връщане
GDPR	Article 30	Processor	Supporting	Записи на обработващия лични данни
GDPR	Article 32; Article 33	Processor	Supporting	Сигурност и уведомяване на администратора за нарушение
GDPR	Article 44	Conditional	Referenced	Маршрутизиране на международни прехвърляния
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Цел, минимизиране, използване, срок за съхранение и ограничаване на разкриването
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Отчетност, информационна сигурност и съответствие
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2	Processor	Supporting	Оценяване на обработващи лични данни, мониторинг, промяна и контроли за съхранение
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23	Processor	Supporting	Приложимост на контролите, оперативен контрол и контроли за доставчици/облак
ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10;	Processor	Supporting	Контроли за доставчици, облак, изтриване, журнализиране и мониторинг

	Control 8.15; Control 8.16			
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Съдействие на клиенти и ограничаване на целите при обработващ лични данни в облачна среда
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Облачно уведомяване за разкриване, записи за разкриване и прозрачност относно подизпълнителите по обработване
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1	Processor	Primary	Облачен интерфейс при нарушения, изход, договорни мерки, поддоговори и записи за местоположения
ISO/IEC 27036- 2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Стратегия и управление на взаимоотношенията по доставка
ISO/IEC 27036- 2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Планиране, споразумение, управление, мониторинг и прекратяване на взаимоотношения с доставчици
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Processor	Supporting	Рамка и документация за изтриване
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Processor	Supporting	Изпълнение на изтриване и изключения

1. Обхват

1.1 Настоящата политика определя задължителните изисквания за поверителност за облачни услуги, при които организацията действа като обработващ лични данни или подизпълнител по обработване, включително SaaS, PaaS, IaaS, хоствано приложение, управляван облак, облачна поддръжка, облачно съхранение, облачни анализи и услуги за облачна инфраструктура, които обработват PII от името на клиенти.

1.2 Настоящата политика се прилага за облачно обработване, извършвано съгласно споразумения с клиенти, документирани нареждания на клиента, нареждания на възходящ обработващ лични данни, договорености с подизпълнители по обработване, конфигурация на облачен регион, достъп за облачна поддръжка, администриране на услуги, резервни копия, репликация, журнализиране, мониторинг, изтриване, връщане, съдействие при нарушения, съдействие при одит и задължения за съдействие на клиенти.

1.3 Настоящата политика обхваща:

1.3.1 обхват на облачното обработване на PII и записи за нареждания;

1.3.2 доказателства за споразумения с клиенти и споделена отговорност;

1.3.3 доказателства за изолация на тенанти, облачен достъп, административен достъп и журнализиране;

1.3.4 управление на подизпълнители по обработване и облачна верига на доставки;

1.3.5 маршрутизиране на местоположение, отдалечен достъп и международни прехвърляния;

1.3.6 доказателства за връщане, прехвърляне, изтриване, унищожаване и изход;

1.3.7 съдействие на клиенти относно права на субекти на данни, DPIA, одити и реагиране при нарушения;

1.3.8 доказателства за мониторинг, изключения, прилагане и подобрение.

1.4 Настоящата политика не създава отделен регистър на клиентски договори, регистър на облачни услуги, регистър за изолация на тенанти, регистър за достъп, регистър на журнали, регистър за изтриване, регистър на заявки за поддръжка, регистър на доказателства за одит, регистър на нарушения, регистър на подизпълнители по обработване или комитет за облачно управление.

1.5 Настоящата политика не заменя:

1.5.1 PII03 относно инвентара на обработването и собствеността върху правните основания;

1.5.2 PII06 относно цялостния работен поток за права на субекти на данни;

1.5.3 PII07 относно методологията за риск за поверителността и DPIA;

1.5.4 PII08 относно контролните точки за защита на личните данни още при проектиране и по подразбиране;

1.5.5 PII09 относно общите контроли за събиране, използване, разкриване и споделяне;

1.5.6 PII10 относно методологията за съхранение, изтриване и унищожаване;

1.5.7 PII12 относно общото управление на жизнения цикъл на обработващи лични данни, подизпълнители по обработване и трети страни;

1.5.8 PII13 относно оценката на механизми за международно прехвърляне;

1.5.9 PII14 относно цялостната архитектура за сигурност и контрол на достъпа до PII;

1.5.10 PII15 относно работния поток за управление на инциденти и нарушения;

1.5.11 PII17 относно контрола на документираната информация;

1.5.12 PII18 относно управлението на мониторинга, одита и подобрението на PIMS.

2. Цел

- 2.1 Целта на настоящата политика е да гарантира, че услугите като обработващ лични данни в облачна среда и като подизпълнител по обработване в облачна среда се предоставят съгласно документирани нареждания на клиента, ясен обхват на обработването, контролирани договорености с подизпълнители по обработване, подходящи отговорности за облачна сигурност, документирано местоположение и маршрутизиране на прехвърляния, задължения за съдействие на клиенти, съдействие при нарушения, възможност за изтриване/връщане и доказателства, годни за одит.
- 2.2 Настоящата политика подпомага готовността за сертификация по ISO/IEC 27701:2025 PIMS за облачни обработващи лични данни и облачни подизпълнители по обработване, като остава интегрирана със съществуващия набор от политики на PIMS и каноничните доказателствени обекти.

3. Цели

3.1 Целите на настоящата политика са да:

- 3.1.1 Дефинира обхвата на облачното обработване на PII преди въвеждане на клиент или съществена промяна.
- 3.1.2 Гарантира, че нарежданията на клиента се записват, преглеждат и изпълняват.
- 3.1.3 Поддържа доказателства за облачен обработващ лични данни и подизпълнител по обработване в каноничните регистри на PIMS.
- 3.1.4 Дефинира доказателства за споделена отговорност, изолация на тенанти, достъп, журнализиране и местоположение, без да се дублира политиката за сигурност на PII.
- 3.1.5 Контролира доказателствата за въвеждане, промяна, прехвърляне на задължения надолу по веригата и мониторинг на подизпълнители по обработване.
- 3.1.6 Подпомага клиентите относно права на субекти на данни, DPIA, искания за одит и реагиране при нарушения.
- 3.1.7 Гарантира, че доказателствата за връщане, изтриване, прехвърляне и унищожаване се съхраняват при изход.
- 3.1.8 Наблюдава контролите за обработващ лични данни в облачна среда и да задейства коригиращи действия чрез REG12.

4. Изисквания на политиката

4.1 Обхват на облачното обработване и нареждания на клиента

- 4.1.1 [Processor] The Privacy Lead / PIMS Manager MUST записва всяка услуга за облачно обработване на PII, ролята на клиента при обработването, източника на нарежданията на клиента, категориите PII, категориите субекти на данни, целта на услугата, местоположението на обработването, зависимостта от подизпълнители по обработване, зависимостта при изтриване и индикатора за прехвърляне в REG02 и REG08 преди въвеждане на клиент или съществена промяна на услугата.
- 4.1.2 [Processor] The Process Owner / Business Owner MUST записва документирани нареждания на клиента за облачно обработване на PII в REG08 преди започване на обработването.
- 4.1.3 [Subprocessor] The Process Owner / Business Owner MUST записва нарежданията на възходящия обработващ лични данни или одобрените от клиента нареждания в REG08 преди обработване на PII като облачен подизпълнител по обработване.
- 4.1.4 [Processor] The Privacy Lead / PIMS Manager MUST записва приложимостта на контролите за обработващ лични данни в облачна среда в REG03 преди нова услуга за облачно обработване на PII да бъде пусната или съществено променена.

- 4.1.5 [Processor] The Data Protection Officer / Privacy Advisor MUST преглежда всяко нареждане на клиента, което изглежда несъвместимо с документираните задължения на клиента, изискванията на PIMS или одобрения обхват на услугата, в REG12 преди организацията да предприеме действие по нареждането.
- 4.1.6 [Processor] The Process Owner / Business Owner MUST записва всяко предложено обработване на клиентски PII извън документираните нареждания на клиента в REG12 и да получава одобрение от Privacy Lead / PIMS Manager преди извършване на обработването.

4.2 Облачна конфигурация, изолация на тенанти, достъп и журнализиране

- 4.2.1 [Processor] The Information Security Lead MUST записва границата на споделената отговорност в облака за достъп до PII, администриране, журнализиране, резервни копия, шифроване, управление на уязвимостите и изтриване в REG08 преди въвеждане на клиент или съществена промяна на услугата.
- 4.2.2 [Processor] The System Owner / Application Owner MUST валидира контролите за изолация на тенанти или за разделяне на клиенти в REG12 преди продукционна употреба и след съществена промяна в архитектурата.
- 4.2.3 [Processor] The System Owner / Application Owner MUST предоставя облачен административен достъп до клиентски PII само след като одобрената служебна необходимост, обхватът на достъпа, продължителността на достъпа и честотата на преглед са записани в REG12.
- 4.2.4 [Processor] The Information Security Lead MUST преглежда привилегирования облачен достъп, достъпа за поддръжка, достъпа до клиентски PII и покритието на журнализирането в REG12 най-малко на тримесечна база.
- 4.2.5 [Processor] The System Owner / Application Owner MUST валидира разделянето на продукционна среда, среди за тестване, тестова среда и среда за поддръжка за клиентски PII в REG12 преди пускане и след съществена промяна на средата.
- 4.2.6 [Processor] The System Owner / Application Owner MUST записва местоположенията на резервни копия, репликация, съхранение на журнали и достъп за поддръжка за облачен клиентски PII в REG02, REG08 или REG09 преди активиране или промяна на тези местоположения.

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Изключения

- 9.1 [Processor] The Process Owner / Business Owner MUST поиска изключение за обработващ лични данни в облачна среда в REG12 преди въвеждане, пускане, подновяване или продължаващо използване, когато изискуемите доказателства за нареждания на клиента, подизпълнител по обработване, местоположение, достъп, журнализиране, изтриване или интерфейс при инциденти са непълни.
- 9.2 [Processor] The Data Protection Officer / Privacy Advisor MUST преглежда исканията за изключение за обработващ лични данни в облачна среда със съществено значение за поверителността в REG12 преди одобрение, когато изключението засяга нареждания на клиента, съдействие за субекти на данни, прехвърляния, подизпълнители по обработване, изтриване, съдействие при нарушения или лични данни с високо въздействие.
- 9.3 [Processor] Top Management MUST одобрява високорискови или съществени изключения за обработващ лични данни в облачна среда в REG12 преди изключението да влезе в сила.

9.4 [Processor] The Privacy Lead / PIMS Manager MUST определя дата на изтичане, собственик на отстраняването, дата за преглед и бележка за остатъчния риск в REG12 за всяко одобрено изключение за обработващ лични данни в облачна среда преди одобрение.

10. Прилагане на политиката

10.1 [Processor] The Privacy Lead / PIMS Manager MUST блокира въвеждането на клиент, пускането на услуга, подновяването или продължаващото обработване, когато изискуеми доказателства в REG02, REG03, REG08, REG09, REG10 или REG12 липсват преди обработването да започне или продължи.

10.2 [Processor] The System Owner / Application Owner MUST деактивира неodobрен облачен достъп, неodobрено използване на регион, неodobрена репликация, неodobрен достъп за поддръжка или неodobрен поток от данни към подизпълнител по обработване в срок до един работен ден след решение за прилагане на политиката и да записва изпълнението в REG08 или REG12.

10.3 [Processor] The Vendor / Procurement Owner MUST спира ново обработване на PII от неodobрен или несъответстващ облачен подизпълнител по обработване, докато доказателствата за коригиращи действия в REG08 не бъдат завършени.

10.4 [Processor] The Incident Response Coordinator MUST ескалира пропуснати срокове за уведомяване на клиенти при инциденти в REG10 и REG12 в срок до един работен ден след идентифициране.

10.5 [Processor] The Internal Audit / Compliance Reviewer MUST проверява ефективността на коригиращите действия за съществени или повторни несъответствия при обработващ лични данни в облачна среда в REG12 в срок до 60 дни след приключване на коригиращото действие.

11. Преглед и поддръжане

11.1 [Processor] The Privacy Lead / PIMS Manager MUST преглежда настоящата политика в REG12 ежегодно и в срок до 30 дни след съществена промяна в задълженията на обработващия лични данни в облачна среда, облачната архитектура, управлението на подизпълнители по обработване, съдействието на клиенти, възможността за изтриване или сертификационните изисквания.

11.2 [Processor] The Vendor / Procurement Owner MUST преглежда записите за облачни подизпълнители по обработване и зависимости от облачни услуги в REG08 най-малко ежегодно и преди подновяване.

11.3 [Processor] The System Owner / Application Owner MUST преглежда доказателствата за изолация на тенанти, привилегирован достъп, журнализиране, резервни копия, репликация и изтриване в REG12 най-малко ежегодно и след съществена промяна в архитектурата.

11.4 [Processor] The Privacy Lead / PIMS Manager MUST преглежда записите в REG09 за облачни местоположения и маршрутизиране на прехвърляния най-малко ежегодно и в срок до 15 работни дни след съществена промяна в местоположение, достъп за поддръжка, резервни копия или подизпълнител по обработване.

11.5 [Processor] The Privacy Lead / PIMS Manager MUST актуализира REG03 в срок до 15 работни дни след одобрени промени в политиката, които засягат приложимостта на контролите за обработващ лични данни в облачна среда.

11.6 [All] Top Management MUST одобрява съществени изменения на настоящата политика в REG12 преди публикуване.

12. Свързани политики

- 12.1 Настоящата политика се подпомага от следните свързани политики:
- 12.2 PII01 - Политика за система за управление на неприкосновеността на личната информация
- 12.3 PII02 - Политика за роли, отговорности и отчетност в областта на поверителността
- 12.4 PII03 - Политика за инвентар на обработването на PII и правно основание
- 12.5 PII06 - Политика за управление на права на субекти на данни
- 12.6 PII07 - Политика за оценка на риска за поверителността и DPIA
- 12.7 PII08 - Политика за защита на личните данни още при проектиране и по подразбиране
- 12.8 PII09 - Политика за събиране, използване, разкриване и споделяне на PII
- 12.9 PII10 - Политика за съхранение, изтриване и унищожаване на PII
- 12.10 PII12 - Политика за управление на поверителността при обработващи лични данни, подизпълнители по обработване и трети страни
- 12.11 PII13 - Политика за международно прехвърляне на PII
- 12.12 PII14 - Политика за сигурност и контрол на достъпа до PII
- 12.13 PII15 - Политика за управление на инциденти и нарушения с PII
- 12.14 PII17 - Политика за документирана информация и управление на доказателства в PIMS
- 12.15 PII18 - Политика за мониторинг, одит и подобрене на PIMS
- 12.16 PII20 - Политика за поверителност на децата
- 12.17 PII21 - Политика за поверителност при AI и автоматизирано вземане на решения
- 12.18 PII22 - Политика за поверителност при маркетинг и бисквитки
- 12.19 PII24 - Политика за CCTV и физическо наблюдение

13. Референтни стандарти и рамки

- 13.1 Настоящата политика е съпоставена със следните стандарти и регулации. Съпоставянето обяснява как политиката подпомага цитираните изисквания и посочва вътрешните клаузи, които ги изпълняват или подпомагат.
- 13.2 ISO/IEC 27701:2025 - Clause 4.1; Clause 6.1.3. Addressed by clauses [4.1.1; 4.1.4; 5.2; 7.1; 11.5].
- 13.3 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.3.1; 4.4.1; 4.6.1; 4.7.1; 4.8.1; 7.1; 7.2; 7.3].
- 13.4 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.5; 4.6.6; 4.8.1; 4.8.2; 4.8.4; 6.1; 6.2; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].
- 13.5 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.2; 4.1.3; 4.1.5; 4.1.6; 4.3.1; 4.7.5; 7.2].
- 13.6 ISO/IEC 27701:2025 - Annex A.2.3.2. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5].
- 13.7 ISO/IEC 27701:2025 - Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].
- 13.8 ISO/IEC 27701:2025 - Annex A.2.5.2; Annex A.2.5.3. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].
- 13.9 ISO/IEC 27701:2025 - Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.3; 4.5.4; 4.7.2; 4.7.5].
- 13.10 ISO/IEC 27701:2025 - Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6].

- 13.11 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.7.3; 5.4; 5.6; 11.3].
- 13.12 GDPR - Article 28. Addressed by clauses [4.1.2; 4.1.3; 4.3.1; 4.3.2; 4.3.4; 4.4.2; 4.4.3; 4.4.5; 4.6.1; 4.6.3; 4.6.5; 4.7.2].
- 13.13 GDPR - Article 30. Addressed by clauses [4.1.1; 4.1.3; 4.4.1; 4.8.1; 7.1].
- 13.14 GDPR - Article 32; Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 7.6].
- 13.15 GDPR - Article 44. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].
- 13.16 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.6; 4.5.1; 4.6.1; 4.6.3].
- 13.17 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.4; 4.3.5; 4.8.1; 4.8.4; 6.1; 8.5; 10.5].
- 13.18 ISO/IEC 29151:2022 - Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2. Addressed by clauses [4.4.1; 4.4.6; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.8.3].
- 13.19 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23. Addressed by clauses [4.1.4; 4.2.1; 4.4.1; 4.4.3; 4.4.6; 4.8.1; 4.8.3; 6.1; 7.1; 11.5].
- 13.20 ISO/IEC 27002:2022 - Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16. Addressed by clauses [4.2.1; 4.2.4; 4.4.1; 4.4.3; 4.4.6; 4.6.1; 4.6.3; 4.7.3; 4.8.3; 11.3].
- 13.21 ISO/IEC 27018:2020 - Annex A.2.1; Annex A.3.1. Addressed by clauses [4.1.2; 4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.5].
- 13.22 ISO/IEC 27018:2020 - Annex A.6.1; Annex A.6.2; Annex A.8.1. Addressed by clauses [4.4.1; 4.4.2; 4.4.5; 4.5.3; 4.5.4].
- 13.23 ISO/IEC 27018:2020 - Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1. Addressed by clauses [4.2.6; 4.4.3; 4.4.4; 4.6.1; 4.6.3; 4.6.5; 4.7.1; 4.7.2; 4.7.5].
- 13.24 ISO/IEC 27036-2:2022 - Clause 6.1.1; Clause 6.1.2. Addressed by clauses [4.1.1; 4.2.1; 4.4.1; 4.4.6; 6.1; 7.2].
- 13.25 ISO/IEC 27036-2:2022 - Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.8.2; 4.8.3; 10.3; 11.2].
- 13.26 ISO/IEC 27555:2025 - Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].
- 13.27 ISO/IEC 27555:2025 - Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7. Addressed by clauses [4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6; 9.1; 9.4].