

		Въведете тук наименованието на регистрираното юридическо лице					
Номер на документа: PII03		Заглавие на документа: Политика за инвентар на обработването на PII и правно основание					
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	Тип покритие	Коментар
ISO/IEC 27701:2025	Clause 4.1	Both	Supporting	Определяне на ролята в PIMS за дейностите по обработване
ISO/IEC 27701:2025	Clause 6.1.2	Both	Supporting	Връзка с тригерите за оценка на риска за поверителността
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Връзка с приложимостта на контролите и SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Документирана информация за инвентара на обработването
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Оперативно планиране и контрол за записите за обработването
ISO/IEC 27701:2025	Clause 8.2	Both	Supporting	Връзка с оперативната оценка на риска за поверителността
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Мониторинг и измерване на инвентара
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Несъответствия в инвентара и коригиращо действие
ISO/IEC 27701:2025	Annex A.1.2.2	Controller	Primary	Идентифициране на целите от администратора
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Primary	Идентифициране на правното основание от администратора
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Supporting	Връзка с проверката за необходимост от DPIA

ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Записи за отговорностите при обработване от съвместни администратори
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Записи на администратора, свързани с обработването на PII
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Записи за договор с клиента и нареждания към обработващия
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Primary	Съответствие на целта на обработващия с нарежданията на клиента
ISO/IEC 27701:2025	Annex A.2.2.7	Processor	Supporting	Записи на обработващия, свързани с обработването на PII
GDPR	Article 5(1)(a)	Controller	Supporting	Връзка със законосъобразност, добросъвестност и прозрачност
GDPR	Article 5(1)(b)	Controller	Supporting	Ограничение на целите
GDPR	Article 5(1)(c)	Controller	Supporting	Минимизиране на данните
GDPR	Article 5(1)(e)	Controller	Supporting	Връзка с ограничението на съхранението
GDPR	Article 5(2)	Controller	Supporting	Доказателства за отчетност
GDPR	Article 6	Controller	Primary	Законосъобразност на обработването
GDPR	Article 9	Conditional	Supporting	Условие за обработване на специални категории данни
GDPR	Article 10	Conditional	Supporting	Условие за данни за присъди и нарушения

GDPR	Article 24	Controller	Supporting	Отговорност и мерки на администратора
GDPR	Article 26	Joint Controller	Supporting	Записи за договорености между съвместни администратори
GDPR	Article 28	Both	Supporting	Записи за нареждания и договор с обработващия
GDPR	Article 30	Both	Primary	Регистър на дейностите по обработване
GDPR	Article 35	Controller	Supporting	Връзка с проверката за необходимост от DPIA
ISO/IEC 29100:2020	Clause 5.3	Both	Supporting	Легитимност и конкретизиране на целта
ISO/IEC 29100:2020	Clause 5.4	Both	Supporting	Ограничение на събирането
ISO/IEC 29100:2020	Clause 5.5	Both	Supporting	Минимизиране на данните
ISO/IEC 29100:2020	Clause 5.6	Both	Supporting	Ограничение на използването, съхранението и разкриването
ISO/IEC 29100:2020	Clause 5.10	Both	Supporting	Отчетност
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Controller	Supporting	Контроли за защита на PII относно цел, събиране, минимизиране, използване, съхранение и разкриване
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Both	Supporting	Връзка с ползите и тригерите за PIA

1. Обхват

1.1 Настоящата политика определя изискванията за поддържане на инвентара на обработването на PII / ROPA и за документиране на правното основание, целите на обработването, ролята при обработване, категориите PII, категориите субекти на данни, получателите, препратките към срокове за съхранение, препратките към трансфери, нарежданията към обработващите, записите за съвместни администратори и връзката с проверката на риска за поверителността.

1.2 Настоящата политика се прилага за:

1.2.1 всички дейности по обработване на PII в обхвата на PIMS;

1.2.2 обработване, извършвано като администратор, съвместен администратор, обработващ или подизпълнител по обработване;

1.2.3 обработване, извършвано чрез бизнес процеси, системи, приложения, доставчици, обработващи, подизпълнители по обработване и получатели при споделяне на данни;

1.2.4 ново обработване, съществено променено обработване и прекратено обработване;

1.2.5 доказателства, поддържани в REG02, и поддържащи доказателства в REG01, REG03, REG04, REG05, REG07, REG08, REG09 и REG12.

1.3 Настоящата политика не заменя подробните контроли за уведомления за поверителност, контролите за съгласие, методологията за DPIA, изпълнението на сроковете за съхранение, избора на механизми за международни трансфери, контролите за договори с обработващи, контролите за сигурност на PII или контролите за документирана информация. Тези изисквания са определени в свързаните политики, посочени в раздел 12.

1.4 За целите на настоящата политика запис в инвентара на обработването означава запис в REG02, който описва отделна дейност по обработване на PII, включително нейната цел, роля, собственик, категории PII, категории субекти на данни, правно основание или препратка към нареждане на клиента, системи, получатели, препратка към срок за съхранение, препратка към трансфер, статус на риска за поверителността и статус на преглед.

1.5 За целите на настоящата политика съществена промяна в обработването означава всяка промяна в целта на обработването, правното основание, ролята в PIMS, категорията PII, категорията субекти на данни, получателя, системата, доставчика, подизпълнителя по обработване, мястото на обработване, трансфера, правилото за съхранение, класификацията на сигурността, уведомлението за поверителност, зависимостта от съгласие, статуса на DPIA, нареждането на клиента или обхвата на сертификация.

2. Цел

2.1 Целта на настоящата политика е да гарантира, че организацията може да идентифицира, документира, обосновава, преглежда и доказва дейностите по обработване на PII в обхвата на PIMS.

2.2 Настоящата политика позволява на организацията да поддържа пълен, актуален и готов за одит инвентар на обработването на PII, който подпомага законосъобразното обработване, отчетността, уведомленията за поверителност, управлението на съгласията, оценката на риска за поверителността, проверката за необходимост от DPIA, сроковете за съхранение, управлението на трансферите, управлението на обработващите и мониторинга на PIMS.

3. Цели

3.1 Целите на настоящата политика са да:

3.1.1 установи REG02 като официален доказателствен обект за инвентара на обработването на PII и ROPA;

- 3.1.2 гарантира, че всяка дейност по обработване на PII има отговорен собственик;
- 3.1.3 разграничи записите за обработване като администратор, съвместен администратор, обработващ и подизпълнител по обработване;
- 3.1.4 документира конкретните цели на обработването преди започване на обработването;
- 3.1.5 документира правното основание за обработване от администратор преди започване на обработването;
- 3.1.6 документира нарежданията на клиента за обработване от обработващ и подизпълнител по обработване преди започване на обработването;
- 3.1.7 документира категориите PII, категориите субекти на данни, получателите, препратките към срокове за съхранение, препратките към трансфери, системите и взаимоотношенията с доставчици;
- 3.1.8 свързва записите в инвентара с доказателства за уведомления за поверителност, съгласия, DPIA, риск, доставчици, трансфери, контроли и одит, когато е приложимо;
- 3.1.9 гарантира, че записите в инвентара на обработването се преглеждат, актуализират и коригират при промени в обработването;
- 3.1.10 избягва създаването на отделни регистри за правни основания или инвентар на обработването извън REG02.

4. Политически изисквания

4.1 Базово състояние на инвентара на обработването

- 4.1.1 [Both] Process Owner / Business Owner MUST създаде запис в инвентара на обработването в REG02 преди започване на всяка нова дейност по обработване на PII.
- 4.1.2 [Both] Process Owner / Business Owner MUST въведе задължителните полета в REG02 за всяка дейност по обработване преди започване на дейността.
- 4.1.3 [Both] Privacy Lead / PIMS Manager MUST одобри задължителния набор от полета в REG02 в REG12 преди първоначалното функциониране на PIMS и ежегодно след това.
- 4.1.4 [Both] Process Owner / Business Owner MUST класифицира ролята на организацията в PIMS за всяка дейност по обработване в REG02 преди започване на дейността.
- 4.1.5 [Both] System Owner / Application Owner MUST свърже всяка система или приложение, обработващи PII, със съответната дейност по обработване в REG02 преди въвеждане на системата в експлоатация.
- 4.1.6 [Both] Vendor / Procurement Owner MUST свърже всяко взаимоотношение с обработващ, подизпълнител по обработване, трета страна за споделяне или съвместен администратор в REG08 със съответната дейност по обработване в REG02 преди одобряване на договора или въвеждане.

4.2 Записи за целите и правното основание на администратора

- 4.2.1 [Controller] Process Owner / Business Owner MUST документира конкретната цел на обработването в REG02 преди PII да се събира, използва, разкрива или обработва по друг начин.
- 4.2.2 [Controller] Privacy Lead / PIMS Manager MUST валидира правното основание, записано в REG02, преди започване на обработване от администратор и преди влизане в сила на всяка промяна на целта.
- 4.2.3 [Controller] Data Protection Officer / Privacy Advisor MUST запише становище в REG12 преди одобряване на ново правно основание за високорисково обработване, специални категории PII, данни за присъди или нарушения, или съществено променено обработване от администратор.

- 4.2.4 [Controller] Process Owner / Business Owner MUST свърже REG02 с REG05, преди обработване от администратор да се основава на съгласие като правно основание.
- 4.2.5 [Controller] Process Owner / Business Owner MUST запише препратката към оценката на легитимния интерес в REG04, преди обработване от администратор да се основава на легитимни интереси.
- 4.2.6 [Conditional] Process Owner / Business Owner MUST запише условието за обработване на специални категории данни в REG02 преди обработване на специални категории PII.
- 4.2.7 [Conditional] Privacy Lead / PIMS Manager MUST запише основанията за разрешаване на обработването на данни за присъди или нарушения в REG02 преди обработване на данни за присъди или нарушения.
- 4.2.8 [Controller] Process Owner / Business Owner MUST документира съвместимостта на целите и проверката на риска за поверителността в REG02 и REG04, преди да използва PII за нова цел, която не е била записана преди това.

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

9. Изключения

9.1 Изключения за инвентара на обработването и правното основание

- 9.1.1 [All] Process Owner / Business Owner MUST поиска изключение в REG12 преди извършване на дейност по обработване на PII без задължително поле в REG02, запис за правно основание, препратка към нареждане на клиента или статус на преглед.
- 9.1.2 [All] Privacy Lead / PIMS Manager MUST оцени въздействието върху поверителността, сертификацията и операциите на всяко изключение, свързано с инвентара на обработването, в REG12 в срок до 10 работни дни от искането.
- 9.1.3 [All] Data Protection Officer / Privacy Advisor MUST запише становище в REG12 преди одобряване на всяко изключение, включващо правно основание, специални категории PII, данни за присъди или нарушения, високорисково обработване, връзка с международен трансфер или ограничение в нареждане на клиента.
- 9.1.4 [All] Top Management MUST одобрява изключения от инвентара на обработването, които надвишават 30 дни, засягат високорисково обработване или засягат обхвата на сертификацията, в REG12 преди изключението да влезе в сила.
- 9.1.5 [All] Privacy Lead / PIMS Manager MUST определи дата на изтичане, която не надвишава 90 дни, в REG12 за всяко одобрено изключение от инвентара на обработването преди одобрението.
- 9.1.6 [All] Process Owner / Business Owner MUST закрие или повторно оцени всяко изключение от инвентара на обработването в REG12 в срок до пет работни дни от изтичането му.

10. Прилагане на политиката

10.1 Прилагане на изискванията за инвентара на обработването и правното основание

- 10.1.1 [All] Privacy Lead / PIMS Manager MUST запише липсващи, неточни, остарели или неодобренни доказателства за инвентара на обработването в REG02 като несъответствие в REG12 в срок до пет работни дни от установяването.
- 10.1.2 [Controller] Process Owner / Business Owner MUST спре ново обработване от администратор, когато задължителните доказателства за цел или правно основание липсват от REG02 преди стартиране.

- 10.1.3 [Processor] Process Owner / Business Owner MUST спре ново обработване от обработващ, когато задължителните доказателства за нареждане на клиента липсват от REG02 или REG08 преди въвеждане на услугата.
- 10.1.4 [Both] System Owner / Application Owner MUST блокира въвеждането на система в експлоатация за обработване на PII, когато липсва задължителната връзка с инвентара в REG02 преди одобрението за въвеждане в експлоатация.
- 10.1.5 [Both] Vendor / Procurement Owner MUST блокира въвеждането на доставчик, обработващ, подизпълнител по обработване, получател от трета страна или съвместен администратор, когато липсват задължителните доказателства за връзка в REG02 и REG08 преди одобряване на договора.
- 10.1.6 [All] Top Management MUST преглежда нерешените съществени несъответствия, свързани с инвентара на обработването или правното основание, в REG12 по време на прегледа от ръководството.
- 10.1.7 [All] Internal Audit / Compliance Reviewer MUST провери ефективността на коригиращите действия за несъответствия в инвентара на обработването в REG12 при следващия планиран одит или в срок до 60 дни от закриването, което от двете настъпи първо.

11. Преглед и поддръжка

11.1 Преглед и поддръжка на политиката

- 11.1.1 [All] Privacy Lead / PIMS Manager MUST преглежда настоящата политика в REG12 ежегодно и в срок до 30 дни от съществена промяна в изискванията към инвентара на обработването, правното основание, нарежданията към обработващите, ROPA или сертификацията.
- 11.1.2 [All] Privacy Lead / PIMS Manager MUST преглежда минималните изисквания към полетата в REG02 в REG12 ежегодно и в срок до 30 дни от съществена правна, регулаторна, договорна или свързана с обработване промяна.
- 11.1.3 [All] Data Protection Officer / Privacy Advisor MUST преглежда съществените за поверителността промени в настоящата политика в REG12 преди одобрение.
- 11.1.4 [All] Top Management MUST одобрява съществени промени в настоящата политика в REG12 преди публикуване.
- 11.1.5 [All] Privacy Lead / PIMS Manager MUST актуализира REG03 и REG04 в срок до 15 работни дни след одобрени промени в политиката, които променят приложимостта на контролите или изискванията за проверка на риска за поверителността.
- 11.1.6 [All] Privacy Lead / PIMS Manager MUST запише комуникирането на одобрените промени в настоящата политика в REG11 в срок до 30 дни от публикуването.

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 PII04 - Политика за уведомления за поверителност и прозрачност
- 12.5 PII05 - Политика за управление на съгласия и предпочитания
- 12.6 PII07 - Политика за оценка на риска за поверителността и DPIA
- 12.7 PII08 - Политика за поверителност 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 PII11 - Политика за точност и качество на PII
- 12.11 PII12 - Политика за управление на поверителността при обработващи, подизпълнители по обработване и трети страни
- 12.12 PII13 - Политика за международен трансфер на PII
- 12.13 PII14 - Политика за сигурност на PII и контрол на достъпа
- 12.14 PII17 - Политика за документирана информация и управление на доказателства в PIMS
- 12.15 PII18 - Политика за мониторинг, одит и подобрене на PIMS

13. Референтни стандарти и рамки

- 13.1 Настоящата политика е съпоставена със следните стандарти и регулации. Съпоставянето обяснява как политиката подпомага цитираните изисквания и идентифицира вътрешните клаузи, които ги прилагат или подпомагат.

13.2 ISO/IEC 27701:2025

- 13.2.1 **Clause 4.1** - Съпоставено с определянето на ролята на организацията в PIMS за всяка дейност по обработване и разграничаването на контексти на администратор, съвместен администратор, обработващ и подизпълнител по обработване. Addressed by clauses [4.1.4; 4.3.1; 4.3.4; 4.3.5].
- 13.2.2 **Clause 6.1.2** - Съпоставено с връзката към тригерите за оценка на риска за поверителността за нови и съществено променени дейности по обработване на PII. Addressed by clauses [4.2.8; 4.5.2; 4.5.3].
- 13.2.3 **Clause 6.1.3** - Съпоставено със свързването на дейностите по обработване с приложимостта на контролите и доказателствата за Декларацията за приложимост на PIMS. Addressed by clauses [4.5.4; 7.1.5; 11.1.5].
- 13.2.4 **Clause 7.5** - Съпоставено с поддържането на записи за инвентар на обработването, правно основание, нареждания към обработващи, прегледи, изключения и коригиращи действия като контролирана документирана информация. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.2; 4.3.1; 4.4.1; 4.5.1; 7.1.1; 7.1.3; 9.1.1; 10.1.1].
- 13.2.5 **Clause 8.1** - Съпоставено с оперативното планиране и контрол за създаване, валидиране, актуализиране, преглеждане и извеждане от употреба на записи в инвентара на обработването преди обработването да започне или да бъде променено. Addressed by clauses [4.1.1; 4.1.5; 4.1.6; 4.5.1; 4.5.6; 7.1.2; 7.1.6; 7.1.7; 7.1.8].
- 13.2.6 **Clause 8.2** - Съпоставено с връзката към оперативната оценка на риска за поверителността от записите в инвентара на обработването и тригерите за съществени промени в обработването. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].
- 13.2.7 **Clause 9.1** - Съпоставено с мониторинга и измерването на пълнотата на инвентара на обработването, валидирането на правното основание, връзката с нарежданията, статуса на прегледите, връзката с проверката за необходимост от DPIA и изключенията при съпоставяне. Addressed by clauses [4.5.4; 4.5.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].
- 13.2.8 **Clause 10.2** - Съпоставено с обработването на несъответствия и изключения, свързани с инвентара и правното основание, коригиращи действия, прилагане на изискванията и проверка на ефективността. Addressed by clauses [9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.6; 10.1.7].

- 13.2.9 **Annex A.1.2.2** - Съпоставено с идентифицирането и документирането на целите на обработване от администратора преди PII да се събира, използва, разкрива или обработва по друг начин. Addressed by clauses [4.1.2; 4.2.1; 4.2.8; 4.3.5].
- 13.2.10 **Annex A.1.2.3** - Съпоставено с определянето, документирането, валидирането и доказването на правното основание за обработване от администратор. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7].
- 13.2.11 **Annex A.1.2.6** - Съпоставено с проверката за необходимост от DPIA на нови и съществено променени дейности по обработване от администратор. Addressed by clauses [4.5.2; 4.5.3; 8.1.5].
- 13.2.12 **Annex A.1.2.8** - Съпоставено със записването на целите на обработване от съвместни администратори и препратките към разпределението на отговорностите. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].
- 13.2.13 **Annex A.1.2.9** - Съпоставено с поддържането на записи на администратора, свързани с обработването на PII, включително цели, категории, получатели, препратки към срокове за съхранение, трансфери, правно основание, проверка на риска, собственик, статус и доказателства за преглед. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.4.6; 4.5.1; 4.5.6; 7.1.2; 7.1.8].
- 13.2.14 **Annex A.2.2.2** - Съпоставено с договора с клиента на обработващия и документираните доказателства за нареждания, включително предмет, продължителност, цел, категории PII и категории субекти на данни. Addressed by clauses [4.3.1; 4.3.2; 5.1.7; 10.1.3].
- 13.2.15 **Annex A.2.2.3** - Съпоставено с гарантирането, че целите на обработване от обработващия остават съгласувани с документираните нареждания на клиента. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 10.1.3].
- 13.2.16 **Annex A.2.2.7** - Съпоставено с поддържането на записи на обработващия, свързани с обработването на PII от името на клиенти. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 8.1.3].

13.3 **GDPR**

- 13.3.1 **Article 5(1)(a)** - Съпоставено с целта на обработването от администратор, валидирането на правното основание и доказателствата за отчетност преди започване на обработването. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.8].
- 13.3.2 **Article 5(1)(b)** - Съпоставено с конкретизирането на целта, оценката на съвместимостта на целта и предотвратяването на обработване за нова недокументирана цел. Addressed by clauses [4.2.1; 4.2.8; 4.3.3].
- 13.3.3 **Article 5(1)(c)** - Съпоставено със записването на категориите PII, категориите субекти на данни и източниците на данни преди обработване с цел подпомагане на прегледа за минимизиране. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].
- 13.3.4 **Article 5(1)(e)** - Съпоставено със записването на правило за съхранение или препратка към срок за съхранение за всяка дейност по обработване. Addressed by clauses [4.4.4; 8.1.6].
- 13.3.5 **Article 5(2)** - Съпоставено с доказателствата за отчетност относно инвентара на обработването, валидирането на правното основание, прегледите, съпоставянето, извадковите одитни проверки и коригиращите действия. Addressed by clauses [4.1.1; 4.2.2; 4.5.4; 4.5.5; 6.1.2; 10.1.1; 10.1.7].
- 13.3.6 **Article 6** - Съпоставено с документирането и валидирането на правното основание за обработване от администратор, включително връзка със съгласие, препратка към оценка

- на легитимния интерес и съвместимост на целта. Addressed by clauses [4.2.2; 4.2.4; 4.2.5; 4.2.8].
- 13.3.7 **Article 9** - Съпоставено със записването на условието за обработване на специални категории данни и становище по поверителност преди обработване на специални категории PII. Addressed by clauses [4.2.3; 4.2.6; 9.1.3].
- 13.3.8 **Article 10** - Съпоставено със записването на основанието за разрешаване на обработването на данни за присъди или нарушения преди обработването. Addressed by clauses [4.2.3; 4.2.7; 9.1.3].
- 13.3.9 **Article 24** - Съпоставено с управлението, прегледа, отчетността и надзора от ръководството на администратора върху инвентара на обработването и записите за правно основание. Addressed by clauses [4.2.2; 5.1.1; 6.1.2; 10.1.6; 11.1.4].
- 13.3.10 **Article 26** - Съпоставено с доказателствата за целта на обработване и разпределението на отговорностите при съвместни администратори. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].
- 13.3.11 **Article 28** - Съпоставено с нареждания към обработващи и подизпълнители по обработване, договор, връзка във взаимоотношението и контроли при въвеждане. Addressed by clauses [4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 5.1.7; 7.1.7; 10.1.3; 10.1.5].
- 13.3.12 **Article 30** - Съпоставено със записите на администратора и обработващия за дейностите по обработване, включително цели на обработването, категории PII, категории субекти на данни, получатели, трансфери, препратки към срокове за съхранение и записи за нареждания на клиента. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.3.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.6; 7.1.2].
- 13.3.13 **Article 35** - Съпоставено с връзката с проверката за необходимост от DPIA при нови, съществено променени или високорискови дейности по обработване от администратор. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].
- 13.4 ISO/IEC 29100:2020**
- 13.4.1 **Clause 5.3** - Съпоставено с легитимността на целта, конкретизирането на целта, връзката с правното основание и доказателствата за съвместимост на целта. Addressed by clauses [4.2.1; 4.2.2; 4.2.8; 4.3.1; 4.3.3].
- 13.4.2 **Clause 5.4** - Съпоставено с ограничението на събирането чрез документиране на категориите PII, категориите субекти на данни, източниците и обосновката преди започване на обработването. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].
- 13.4.3 **Clause 5.5** - Съпоставено с минимизирането на данните чрез изисквания към полетата на инвентара, документиране на категориите, документиране на получателите и преглед на актуалните записи за обработване. Addressed by clauses [4.1.2; 4.4.1; 4.4.2; 4.5.4; 8.1.6].
- 13.4.4 **Clause 5.6** - Съпоставено с ограничението на използването, съхранението, разкриването и трансфера чрез документираните цели, категории получатели, препратки към срокове за съхранение, връзка с трансфери и контроли при промяна на целта. Addressed by clauses [4.2.1; 4.2.8; 4.4.2; 4.4.4; 4.4.5].
- 13.4.5 **Clause 5.10** - Съпоставено с отчетността чрез собственост, управление на инвентара, преглед, съпоставяне, извадкови одитни проверки, обработване на изключения и доказателства за коригиращи действия. Addressed by clauses [4.1.1; 4.1.3; 4.5.4; 4.5.5; 5.1.5; 6.1.1; 8.1.1; 10.1.1].
- 13.5 ISO/IEC 29151:2022**

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Съпоставено с контролите за защита на PII относно легитимност на целта, ограничение на събирането, минимизиране на данните и ограничение на използването, съхранението и разкриването. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.4; 4.4.6; 4.5.4; 8.1.6].

13.6 ISO/IEC 29134:2020

13.6.1 **Clause 5.1; Clause 6.2** - Съпоставено с използването на промени в инвентара на обработването като тригер за оценка на риска за поверителността и проверка за необходимост от DPIA, преди ново или съществено променено обработване да продължи. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].