

				Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII11				Заглавие на документа: Политика за точност и качество на PII							
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. Никоя 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 7.5; Clause 8.1	Both	Primary	Документирани доказателства за точност и оперативен контрол
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Мониторинг, несъответствие и коригиращо действие
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Записи за обработване от администратора
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.7	Controller	Primary	Задължения за точност и механизми за коригиране
ISO/IEC 27701:2025	Annex A.1.3.8	Controller	Primary	Уведомяване за корекция до съответните получатели
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Нареждания към обработващия лични данни, съдействие и записи
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Съдействие от обработващия лични данни при корекции
GDPR	Article 5(1)(d); Article 5(2)	Controller	Primary	Точност и отчетност
GDPR	Article 16	Controller	Primary	Коригиране
GDPR	Article 19	Controller	Primary	Уведомяване на получателите
GDPR	Article 24	Controller	Supporting	Мерки на администратора
GDPR	Article 28	Both	Supporting	Съдействие от обработващия лични данни и нареждания
GDPR	Article 30	Both	Supporting	Записи за обработването

ISO/IEC 29100:2020	Clause 5.7	Both	Primary	Принцип на точност и качество
ISO/IEC 29151:2022	Annex A.8	Both	Primary	Контроли за точност и качество на PII

1. Обхват

1.1 Тази политика определя изискванията за поддържане на точността, пълнотата, актуалността, адекватността и относимостта на PII, обработвана в обхвата на PIMS.

1.2 Тази политика се прилага в контекстите на администратор, съвместен администратор, обработващ лични данни и подизпълнител по обработване. Задълженията на администратора са основни. Задълженията на обработващия лични данни и подизпълнителя по обработване се прилагат, когато организацията подпомага коригирането, синхронизацията или свързаните с точността нареждания на администратора.

1.3 Тази политика обхваща:

1.3.1 отговорност за точността по дейност по обработване;

1.3.2 проверки на точността при събиране, импортиране, промяна на източника и точки за преглед;

1.3.3 критерии за задействане на корекция и валидиране;

1.3.4 преглед на остарели данни за записи с високо въздействие;

1.3.5 синхронизация на одобрени корекции в съответните системи и към последващи страни;

1.3.6 съдействие при корекции от обработващи лични данни и подизпълнители по обработване;

1.3.7 доказателства в REG02, REG06, REG08 и REG12.

1.4 Тази политика не въвежда отделна програма за качество на данните, регистър за качество на данните, функция за управление на основни данни, рамка за качество на аналитични данни или рамка за качество на данни за обучение на AI.

1.5 Тази политика не заменя:

1.5.1 PII03 относно инвентара на обработването, целите, правното основание и собствеността върху REG02;

1.5.2 PII06 относно приемането на искания за упражняване на права от субект на данни, проверката на идентичността, обработването на отговорите в законоустановен срок и комуникациите при приключване;

1.5.3 PII10 относно изпълнението на съхранение, заличаване, изтриване и унищожаване;

1.5.4 PII12 относно управлението на жизнения цикъл на обработващи лични данни, подизпълнители по обработване и трети страни;

1.5.5 PII14 относно сигурността на PII и контролите за достъп;

1.5.6 PII18 относно мониторинга, одита, несъответствията, коригиращите действия и управлението на подобренията на ниво PIMS.

1.6 За целите на тази политика запис с високо въздействие е запис на PII, използван за предоставяне, отказ, изменение или съществено засягане на достъпа до услуга, договор, трудовоправен въпрос, финансов резултат, резултат, свързан със здравето, решение относно допустимост, решение относно идентичност, решение относно риск или друго решение, при което неточна PII може съществено да засегне субект на данни.

2. Цел

2.1 Целта на тази политика е да гарантира, че PII, използвана от организацията, остава точна и подходяща за целите на обработването, записани в PIMS, както и че неточната, непълната, остарялата или оспорената PII се коригира, синхронизира или ескалира чрез контролирани доказателства.

3. Задачи

3.1 Задачите на тази политика са да:

- 3.1.1 възложи отговорността за точността за всяка съответна дейност по обработване;
- 3.1.2 определи оптимизирани и проверими проверки на точността, без да създава отделна програма за управление на данните;
- 3.1.3 установи ясни критерии за задействане на корекция, преглед на остарели данни и синхронизация;
- 3.1.4 подпомага исканията за корекция от субект на данни, без да дублира работния процес за искания за упражняване на права;
- 3.1.5 подпомага съдействието от обработващи лични данни и подизпълнители по обработване при корекции съгласно документирани нареждания;
- 3.1.6 съхранява доказателства в REG02, REG06, REG08 и REG12;
- 3.1.7 ескалира повтарящи се, просрочени или с високо въздействие проблеми с точността чрез процеса на PIMS за коригиращи действия.

4. Изявления на политиката

4.1 Отговорност за точността и изисквания за точност

- 4.1.1 [Controller] Process Owner / Business Owner трябва да запише отговорника за точността, официалния източник, флага за запис с високо въздействие и честотата на преглед на точността за всяка дейност по обработване като администратор в REG02 преди започване на обработването и в срок до 10 работни дни след съществена промяна в обработването.
- 4.1.2 [Joint Controller] Vendor / Procurement Owner трябва да запише разпределението на отговорността за точността между съвместните администратори в REG08 и да го свърже със засегнатата дейност по обработване в REG02 преди започване на обработването като съвместни администратори.
- 4.1.3 [Processor] Vendor / Procurement Owner трябва да запише задълженията за съдействие при корекции за клиента и разрешения канал за нареждания в REG08 преди въвеждане на услуга на обработващ лични данни и в срок до 10 работни дни след съществена промяна в договора.
- 4.1.4 [Both] Process Owner / Business Owner трябва да определи минимални проверки на точността за всяка категория PII, използвана във възложена дейност по обработване, в REG02 преди започване на обработването и ежегодно след това.
- 4.1.5 [Controller] Process Owner / Business Owner трябва да класифицира записите с високо въздействие в REG02 преди започване на обработването като администратор и ежегодно след това.
- 4.1.6 [Both] Privacy Lead / PIMS Manager трябва да преглежда на тримесечна база отговорността за точността в REG02, флагите за високо въздействие и периодичността на прегледите и да записва неотстранените пропуски в REG12 в срок до пет работни дни след приключване на прегледа.

4.2 Проверки на точността и преглед на остарели данни

- 4.2.1 [Controller] Process Owner / Business Owner трябва да запише приключването на определената проверка на точността в REG02, преди новосъбраната PII да бъде използвана за активно обработване от администратора.
- 4.2.2 [Controller] Process Owner / Business Owner трябва да провери надеждността на PII, събрана от източник, различен от субекта на данни, в REG02 преди първото използване и преди всяка съществена промяна на източника.

- 4.2.3 [Both] Process Owner / Business Owner трябва да преглежда активните записи с високо въздействие в REG02 най-малко ежегодно и преди да се позове на запис с високо въздействие, чиято дата за преглед е просрочена.
- 4.2.4 [Both] System Owner / Application Owner трябва да идентифицира индикатори за остарели данни за системни записи с високо въздействие в REG02 преди въвеждане на системата в експлоатация и в срок до 30 дни след съществена промяна в системата.
- 4.2.5 [Both] Process Owner / Business Owner трябва да запише вътрешен проблем с точността в REG12 в срок до пет работни дни, когато проверка на точността установи неточна, непълна, остаряла, несъгласувана или неподкрепена PII, която не е повдигната като искане за корекция от субект на данни.
- 4.2.6 [Controller] Privacy Lead / PIMS Manager трябва да свърже всяко искане за корекция, произхождащо от субект на данни, в REG06 със засегнатата дейност по обработване в REG02 в срок до пет работни дни след възлагането за съществен преглед на точността.

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

9. Изключения

9.1 Изключения относно точността

- 9.1.1 [Both] Process Owner / Business Owner трябва да поиска изключение относно точността в REG12 преди използване на известна непроверена, остаряла или оспорена PII извън записаната честота на преглед.
- 9.1.2 [Both] Privacy Lead / PIMS Manager трябва да оцени въздействието и мерките за смекчаване за всяко изключение относно точността в REG12 в срок до пет работни дни от искането.
- 9.1.3 [Conditional] Data Protection Officer / Privacy Advisor трябва да запише становище в REG12 преди одобряване на изключение относно точността, което включва записи с високо въздействие, оспорена корекция или правно изискване.
- 9.1.4 [All] Top Management трябва да одобри изключение относно точността, което засяга записи с високо въздействие, неразрешени корекции, сертификационен обхват или правни задължения, в REG12 преди изключението да влезе в сила.
- 9.1.5 [Both] Privacy Lead / PIMS Manager трябва да определи дата на изтичане, която не надвишава 90 дни, в REG12 за всяко одобрено изключение относно точността преди одобрението.
- 9.1.6 [Both] Privacy Lead / PIMS Manager трябва да приключи или преоцени всяко изключение относно точността в REG12 в срок до пет работни дни след изтичането му.

10. Прилагане на политиката

10.1 Прилагане на политиката и обработване на несъответствия

- 10.1.1 [Both] Privacy Lead / PIMS Manager трябва да запише просрочен преглед с високо въздействие, некоригирана неточна PII или пропуснатата синхронизация като несъответствие в REG12 в срок до пет работни дни от идентифицирането.
- 10.1.2 [Both] System Owner / Application Owner трябва да предотврати въвеждането в експлоатация на система, обработваща PII с високо въздействие, когато в REG02 липсва изискваният отговорник за точността, метод за проверка на точността или път за корекция, и да запише решението в REG12 преди въвеждане в експлоатация.
- 10.1.3 [Controller] Process Owner / Business Owner трябва да спре позоваването на известна неточна PII с високо въздействие за съществени решения, докато корекция, ограничение или одобрено изключение не бъдат записани в REG06 или REG12.

- 10.1.4 [Both] Vendor / Procurement Owner трябва да ескалира неуспех на обработващ лични данни, подизпълнител по обработване или получател да съдейства за одобрена корекция в REG08 и REG12 в срок до пет работни дни след крайния срок за съдействие.
- 10.1.5 [All] Top Management трябва да изиска коригиращо действие в REG12 в срок до 10 работни дни при повторен или продължителен неуспех относно точността с високо въздействие.
- 10.1.6 [All] Internal Audit / Compliance Reviewer трябва да провери ефективността на коригиращото действие за несъответствия относно точността на PII в REG12 при следващия планиран одит на PIMS или в срок до 60 дни от приключването, което от двете настъпи първо.

11. Преглед и поддръжка

11.1 Преглед на политиката и контролите за точност

- 11.1.1 [All] Privacy Lead / PIMS Manager трябва да преглежда тази политика в REG12 ежегодно и в срок до 30 дни след съществена правна промяна, промяна в обработването, системата или сертификационния обхват.
- 11.1.2 [Both] Process Owner / Business Owner трябва да преглежда отговорността за точността, класификацията с високо въздействие и периодичността на прегледите в REG02 ежегодно и в срок до 30 дни след съществена промяна в обработването.
- 11.1.3 [Both] System Owner / Application Owner трябва да преглежда пътя за корекция и процедурата за синхронизация, записани в REG02, ежегодно и в срок до 30 дни след съществена промяна в системата.
- 11.1.4 [Both] Vendor / Procurement Owner трябва да преглежда задълженията за съдействие при корекции от обработващи лични данни, подизпълнители по обработване, получатели и страни по споделяне на данни в REG08 преди подновяване и в срок до 30 дни след съществена промяна в отношенията.
- 11.1.5 [Conditional] Data Protection Officer / Privacy Advisor трябва да прегледа въздействието върху поверителността на съществени промени в политиката в REG12 преди одобрение.
- 11.1.6 [All] Top Management трябва да одобри съществени промени в тази политика в REG12 преди публикуване.

12. Свързани политики

- 12.1 PII01 - Политика за система за управление на неприкосновеността на личната информация
- 12.2 PII02 - Политика за роли, отговорности и отчетност в областта на поверителността
- 12.3 PII03 - Политика за инвентар на обработването на PII и правно основание
- 12.4 PII06 - Политика за управление на правата на субектите на данни
- 12.5 PII08 - Политика за поверителност още при проектиране и по подразбиране
- 12.6 PII09 - Политика за събиране, използване, разкриване и споделяне на PII
- 12.7 PII10 - Политика за съхранение, изтриване и унищожаване на PII
- 12.8 PII12 - Политика за управление на поверителността при обработващи лични данни, подизпълнители по обработване и трети страни
- 12.9 PII14 - Политика за сигурност и контрол на достъпа до PII
- 12.10 PII17 - Политика за документирана информация и управление на доказателства в PIMS
- 12.11 PII18 - Политика за мониторинг, одит и подобрене на PIMS

13. Референтни стандарти и рамки

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Съпоставено с документиран изисквания за точност, доказателства в REG02 и REG06, работен процес за корекция, работен процес за синхронизация, отговорности за внедряване и оперативни контроли. 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** - Съпоставено с мониторинг на точността, показатели, записване на несъответствия, коригиращо действие, ескалация, извадкова проверка при одит и проверка на ефективността. 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** - Съпоставено със записи за обработване от администратора, отговорност за точността, източник, класификация с високо въздействие, честота на преглед и актуализации на 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** - Съпоставено с определяне и изпълнение на задълженията на администратора за корекция, валидиране, одобрение на корекция, внедряване на корекция, обработване на спорове и доказателства за приключване. 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** - Съпоставено с уведомяване на съответните последващи страни и проследяване на потвържденията за одобрени корекции. 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** - Съпоставено с доказателства за клиентско споразумение с обработващ лични данни, задължения за съдействие при корекции за клиента, разрешени канали за нареждания и записи на обработващия лични данни. 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** - Съпоставено със средства на обработващия лични данни за подпомагане на задълженията на администратора за корекция съгласно документирано нареждане. 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)** - Съпоставено с отговорност за точността, проверки, преглед на остарели данни, корекция, синхронизация, доказателства, мониторинг и записи за отчетност. 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** - Съпоставено с валидиране, одобрение, внедряване и приключване на позиции за корекция, записани в REG06 и 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** - Съпоставено с уведомяване за корекции до получатели, обработващи лични данни и последващи страни и проследяване на потвържденията. 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** - Съпоставено с мерки на администратора, отговорност, управленски преглед, изключения, ескалация и коригиращо действие за контролите за точност. 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** - Съпоставено със съдействие при корекции от обработващи лични данни и подизпълнители по обработване, документирани нареждания, разрешено от клиента внедряване и ескалация на неуспехи при съдействие. 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** - Съпоставено със записи за обработването, използвани за доказване на отговорност за точността, източници, класификации с високо въздействие, системни връзки и актуализации на дейностите по обработване. 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** - Съпоставено с очакванията за точност и качество за точна, пълна, актуална, адекватна и относима PII, включително надеждност на източника, валидиране на корекции и периодични проверки. 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** - Съпоставено с контроли за точност и качество на PII за процедури за събиране, надеждност на източника, валидиране, периодичен преглед, корекция и механизми за актуализация с високо въздействие. 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].