					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII10					Заглавие на документа: **Политика за съхранение, изтриване и унищожаване 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**

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/контрол/член	Приложимост	Вид покритие	Коментар
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Документирани доказателства за съхранение 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.1.2.8; Annex A.1.2.9	Controller / Joint Controller	Supporting	Съвместна отговорност и записи за обработването
ISO/IEC 27701:2025	Annex A.1.3.7; Annex A.1.3.8	Controller	Supporting	Поддръжка за изпълнение на изтриване
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Съхранение, изтриване и унищожаване
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Нареждания на клиента и записи на обработващия лични данни
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3	Processor	Primary	Поддръжка за изтриване и способност за унищожаване
ISO/IEC 27701:2025	Annex A.3.20; Annex A.3.21; Annex A.3.24	Both	Supporting	Унищожаване на носители и обработване на резервни копия
GDPR	Article 5(1)(e); Article 5(2)	Controller	Primary	Ограничение на съхранението и отчетност
GDPR	Article 17	Controller	Supporting	Поддръжка за изпълнение на изтриване
GDPR	Article 24	Controller	Supporting	Мерки на администратора
GDPR	Article 26	Joint Controller	Supporting	Разпределение на съвместната отговорност

GDPR	Article 28	Processor	Supporting	Изтриване и връщане от обработващия лични данни
GDPR	Article 30	Both	Supporting	Записи за обработването
GDPR	Article 32	Both	Supporting	Сигурно обработване и поддръжка за унищожаване
ISO/IEC 29100:2020	Clause 5.5; Clause 5.6; Clause 5.10	Both	Supporting	Минимизиране, ограничение на срока за съхранение и отчетност
ISO/IEC 29151:2022	Annex A.7; Annex A.7.2	Both	Supporting	Контроли за съхранение и изтриване на временни файлове
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	Both	Primary	Рамка за изтриване и документация
ISO/IEC 27555:2025	Clause 7.2; Clause 7.3; Clause 8.3	Controller	Primary	Срокове за изтриване и правила 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	Both	Primary	Внедряване и изключения
ISO/IEC 27555:2025	Clause 10.1; Clause 10.2; Clause 10.3	Both	Primary	Отговорности и управление на внедряването
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Интегриране на риска за поверителността
ISO/IEC 27002:2022	Control 7.14; Control 8.10	Both	Supporting	Сигурно унищожаване и изтриване на информация

1. Обхват

1.1 Настоящата политика определя изискванията на организацията за дефиниране, преглед, изпълнение и доказване на съхранението, изтриването, анонимизацията, деидентификацията, връщането, прехвърлянето и унищожаването на PII.

1.2 Настоящата политика се прилага за PII, обработвана в контекст на администратор, съвместен администратор, обработващ лични данни и подизпълнител по обработване, включително PII, съхранявана в работещи системи, архиви, резервни копия, реплики, журнали, среди за тестване, временни файлове, хартиени записи и носители за съхранение.

1.3 Настоящата политика се прилага за задължения за съхранение и изтриване, произтичащи от одобрени цели на обработването, записи за правно основание, нареждания на администратор, договорни изисквания, резултати от искания за изтриване на субект на данни, изход от услуга, унищожаване на носители за съхранение и констатации от мониторинг на PIMS.

1.4 Настоящата политика не определя избора на правно основание, съдържанието на уведомление за поверителност, цялостното обработване на правата на субекта на данни, управлението на жизнения цикъл на обработващия лични данни, механизмите за международно прехвърляне, архитектурата на контролите за сигурност, работния поток за реагиране при инциденти или методологията за одит на PIMS. Тези контроли са уредени в свързаните политики.

1.5 За целите на настоящата политика съществена промяна означава всяка промяна в целта на обработването, категорията PII, категорията субект на данни, мястото на системно съхранение, закона или договора относно съхранението, нареждането на клиента, архитектурата на резервните копия, подхода за архивиране, метода за унищожаване, договорността с обработващ лични данни или подизпълнител по обработване, работния поток за изтриване или обхвата на сертификацията на PIMS, която засяга съхранението, изтриването или унищожаването.

2. Цел

2.1 Целта на настоящата политика е да гарантира, че PII се съхранява само за одобрени цели и срокове, изтрива се или по друг начин се унищожава, когато вече не е необходима, и е подкрепена с доказателства, годни за одит.

2.2 Настоящата политика позволява на организацията да демонстрира ограничение на съхранението, отчетно управление на съхранението, контролирано изпълнение на изтриване, сигурно унищожаване, съгласуване с нарежданията към обработващия лични данни, контрол на изключенията и непрекъснато подобрение, без да създава отделен регистър за изтриване.

3. Цели

3.1 Целите на настоящата политика са да:

3.1.1 определят собствеността върху правилата за съхранение и необходимите метаданни за съхранение;

3.1.2 гарантират, че правилата за съхранение се записват в инвентара на обработването на PII / ROPA;

3.1.3 гарантират, че действията по изтриване от обработващи лични данни и подизпълнители по обработване се основават на нареждане на клиента или договор;

3.1.4 гарантират, че PII с изтекъл срок се изтрива, връща, прехвърля, анонимизира, деидентифицира или унищожава чрез одобрени методи;

3.1.5 разграничат работещи системи, архиви, резервни копия, реплики, журнали, среди за тестване и временни файлове;

3.1.6 гарантират, че доказателствата за изтриване и унищожаване се съхраняват в канонични доказателствени обекти на PIMS;

3.1.7 гарантират, че изключенията от съхранението са ограничени във времето, одобрени и преглеждани;

3.1.8 интегрират мониторинга на съхранението и изтриването с несъответствията, коригиращите действия и подобренията.

4. Изявления на политиката

4.1 Възлагане на правила за съхранение

4.1.1 [Controller] Process Owner / Business Owner трябва да възложи документирано правило за съхранение на всяка дейност по обработване в качеството на администратор в REG02 преди започване на дейността по обработване.

4.1.2 [Joint Controller] Process Owner / Business Owner трябва да запише разпределението на отговорностите за съхранение и изтриване между съвместните администратори в REG02 и REG08 преди започване или промяна на съвместното обработване.

4.1.3 [Processor] Vendor / Procurement Owner трябва да запише нарежданията на клиента за съхранение, връщане, прехвърляне или изтриване за дейности на обработващ лични данни в REG08 преди започване или промяна на обработването от обработващия лични данни.

4.1.4 [Subprocessor] Vendor / Procurement Owner трябва да запише изискванията за пренасяне към подизпълнител по обработване относно съхранение, връщане, прехвърляне или изтриване в REG08 преди въвеждане на подизпълнителя по обработване или промяна на нареждането.

4.1.5 [Both] Privacy Lead / PIMS Manager трябва да провери, че всяко одобрено правило за съхранение в REG02 включва срока за съхранение, началния тригер, собственика, обосновката, окончателното действие и датата на следващ преглед, преди правилото да бъде одобрено.

4.1.6 [Both] Data Protection Officer / Privacy Advisor трябва да запише становище в REG02 или REG12 преди одобряване на всяко правило за съхранение, което включва правен конфликт, високорисково обработване, PII от специална категория или съхранение извън първоначалната цел на обработването.

4.2 Преглед и ограничение на съхранението

4.2.1 [Both] Process Owner / Business Owner трябва да преглежда възложените правила за съхранение в REG02 най-малко веднъж годишно и в срок до 30 дни от съществена промяна.

4.2.2 [Both] Privacy Lead / PIMS Manager трябва да одобри или отхвърли нови или променени правила за съхранение в REG02 в срок до 10 работни дни от подаването им.

4.2.3 [Both] System Owner / Application Owner трябва да потвърди техническия или ръчния метод за прилагане на всяко правило за съхранение в REG02 преди въвеждане в продукционна експлоатация и при всеки годишен преглед на съхранението.

4.2.4 [Controller] Process Owner / Business Owner трябва да ограничи активното използване на PII, съхранявана само по правни, договорни, одитни или спорни причини, в REG02 в срок до пет работни дни от установяване на условието за ограничение.

4.2.5 [Both] Privacy Lead / PIMS Manager трябва да запише нерешен риск от прекомерно съхранение или просрочен преглед на съхранението в REG12 в срок до пет работни дни от установяването.

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

9. Изключения

9.1.1 [All] Process Owner / Business Owner трябва да подава всяко искане за съхраняване на PII извън одобреното правило за съхранение в REG12 преди изключението да стане активно.

9.1.2 [All] Privacy Lead / PIMS Manager трябва да одобри или отхвърли исканията за изключение от съхранението в REG12 преди изключението да стане активно.

9.1.3 [All] Data Protection Officer / Privacy Advisor трябва да запише становище в REG12 преди одобряване на всяко изключение, което включва правен конфликт, отказ за изтриване, високорискова PII, външно споделяне или въздействие върху сертификацията.

9.1.4 [All] Top Management трябва да одобри в REG12 изключения от съхранението, надвишаващи 90 дни, засягащи високорисково обработване или засягащи външно уверение, преди изключението да стане активно.

9.1.5 [All] Privacy Lead / PIMS Manager трябва да определи собственик, дата на изтичане, компенсиращ контрол и честота на преглед в REG12 за всяко одобрено изключение от съхранение, изтриване или унищожаване.

9.1.6 [All] Privacy Lead / PIMS Manager трябва да преглежда всяко открито изключение в REG12 най-малко ежемесечно до закриването му.

9.1.7 [All] Process Owner / Business Owner трябва да закрие или поднови всяко изключение в REG12 преди датата на изтичане на изключението.

10. Прилагане на политиката

10.1.1 [All] Privacy Lead / PIMS Manager трябва да запише несъответствие в REG12 в срок до пет работни дни от установяване на липсващи метаданни за съхранение, просрочен преглед на съхранението, неподкрепено съхранение, пропуснато действие по окончателно действие или липсващи доказателства.

10.1.2 [All] System Owner / Application Owner трябва да спре новото продукционно използване на дейност по обработване в REG12, когато необходимите технически контроли за съхранение липсват преди въвеждане в експлоатация.

10.1.3 [All] Process Owner / Business Owner трябва да прекрати неодобрено активно използване на PII, съхранявана само по правни, договорни, одитни или спорни причини, в срок до пет работни дни и да запише действието в REG02 или REG12.

10.1.4 [Processor] Vendor / Procurement Owner трябва да ескалира просрочени насочени от клиента действия по окончателно действие в REG08 и REG12 в срок до пет работни дни от пропуснатия договорен срок.

10.1.5 [Subprocessor] Vendor / Procurement Owner трябва да ескалира липсващи доказателства за окончателно действие от подизпълнител по обработване в REG08 и REG12 в срок до пет работни дни от пропуснатия договорен срок за доказателства.

10.1.6 [All] Internal Audit / Compliance Reviewer трябва да провери ефективността на коригиращите действия за несъответствия при съхранение, изтриване и унищожаване в REG12 при следващия планиран одит или в срок до 60 дни от закриването, което от двете настъпи първо.

10.1.7 [Conditional] Incident Response Coordinator трябва да инициира обработване в REG10, когато несъответствие при съхранение, изтриване или унищожаване показва подозрение за инцидент с PII.

11. Преглед и поддръжка

11.1.1 [All] Privacy Lead / PIMS Manager трябва да преглежда настоящата политика ежегодно и да записва резултата от прегледа в REG12.

11.1.2 [All] Privacy Lead / PIMS Manager трябва да прегледа настоящата политика в срок до 30 дни от съществена промяна в закона за съхранение, целта на обработването, нареждане към обработващ лични данни, системната архитектура, архитектурата на резервните копия, подхода за архивиране, работния поток за изтриване, процеса на унищожаване или изискванията за сертификация на PIMS.

11.1.3 [All] Data Protection Officer / Privacy Advisor трябва да прегледа съществените за поверителността промени в настоящата политика в REG12 преди одобрение.

11.1.4 [All] Top Management трябва да одобрява съществени промени в настоящата политика в REG12 преди публикуване.

11.1.5 [All] Privacy Lead / PIMS Manager трябва да запише комуникацията на одобрените промени в политиката в REG11 в срок до 30 дни от публикуването.

12. Свързани политики

12.1 Настоящата политика се подкрепя 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 PII04 - Политика за уведомление за поверителност и прозрачност

12.6 PII06 - Политика за управление на правата на субектите на данни

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 PII12 - Политика за управление на поверителността при обработващи лични данни, подизпълнители по обработване и трети страни

12.10 PII14 - Политика за сигурност на PII и контрол на достъпа

12.11 PII15 - Политика за управление на инциденти и нарушения, свързани с PII

12.12 PII17 - Политика за документирана информация и управление на доказателства в PIMS

12.13 PII18 - Политика за мониторинг, одит и подобрение на PIMS

13. Референтни стандарти и рамки

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Съпоставено с документирани доказателства за съхранение, оперативно планиране, метаданни за съхранение, доказателства за внедряване и записи за изпълнение на жизнения цикъл. Addressed by clauses [4.1.5; 4.2.3; 4.3.5; 4.4.1; 7.1.1; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Съпоставено с мониторинг, показатели, преглед на просрочени действия, несъответствие и коригиращо действие за контролите за

съхранение, изтриване и унищожаване. Addressed by clauses [4.2.5; 6.1.1; 6.1.2; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 10.1.1; 10.1.6].

13.2.3 **Annex A.1.2.8; Annex A.1.2.9** - Съпоставено с доказателства за отговорност на съвместните администратори и записи за обработване от администратора, съдържащи метаданни за съхранение и окончателно действие. Addressed by clauses [4.1.1; 4.1.2; 4.1.5; 4.2.1; 6.1.4; 7.1.2].

13.2.4 **Annex A.1.3.7; Annex A.1.3.8** - Съпоставено с поддръжка за изпълнение на изтриване, маршрутизиране на оценка за изтриване и връзка с доказателства от трети страни, когато резултатите от изтриване изискват действие. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.2.5 **Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9** - Съпоставено с изтриване или деидентификация в края на обработването, обработване на временни файлове, ограничение на съхранението и документирани контроли за окончателно действие. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.2.4; 4.3.1; 4.3.5; 4.3.6; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Съпоставено с клиентски споразумения на обработващия лични данни, документирани цели на клиента и записи за обработването от обработващия лични данни. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7].

13.2.7 **Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3** - Съпоставено с поддръжка от обработващия лични данни за задълженията на клиента, обработване на временни файлове и способност за връщане, прехвърляне или окончателно действие. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 10.1.4; 10.1.5].

13.2.8 **Annex A.3.20; Annex A.3.21; Annex A.3.24** - Съпоставено с обработване на жизнения цикъл на носителите за съхранение, проверки при повторна употреба или освобождаване на оборудване и обработване на резервни копия за PII. Addressed by clauses [4.3.6; 4.3.7; 4.4.1; 4.4.3; 4.4.4; 4.4.6; 5.1.4].

13.3 GDPR

13.3.1 **Article 5(1)(e); Article 5(2)** - Съпоставено с ограничение на съхранението, отчетност за съхранението, одобрени метаданни за съхранение, доказателства и преглед. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 4.2.4; 4.3.1; 4.3.5; 6.1.1; 8.1.1; 8.1.2; 10.1.1].

13.3.2 **Article 17** - Съпоставено с маршрутизиране на одобрен резултат от изтриване, доказателства за изпълнение и ескалация на инцидент, когато отказите на контроли за изтриване показват подозрение за инцидент с PII. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.3.3 **Article 24** - Съпоставено с управление от администратора, мерки за отчетност, прегледи, изключения, коригиращи действия и поддръжка на политиката. Addressed by clauses [4.1.6; 6.1.2; 6.1.3; 9.1.2; 9.1.3; 9.1.4; 11.1.1; 11.1.2; 11.1.4].

13.3.4 **Article 26** - Съпоставено с разпределение на отговорностите за съхранение и изтриване между съвместните администратори. Addressed by clauses [4.1.2; 6.1.4].

13.3.5 **Article 28** - Съпоставено със съгласуване на нарежданията към обработващи лични данни и подизпълнители по обработване, връщане, прехвърляне, окончателно действие, доказателства и ескалация. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7; 10.1.4; 10.1.5].

13.3.6 **Article 30** - Съпоставено с метаданни за съхранение и окончателно действие в записите за обработване за дейности на администратор и обработващ лични данни. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.2.1; 4.4.1; 7.1.2].

13.3.7 **Article 32** - Съпоставено със сигурно оперативно обработване на съхранявана PII, техническо прилагане, контрол на носители за съхранение, обработване на резервни копия и ескалация на инциденти. Addressed by clauses [4.2.3; 4.3.6; 4.4.3; 4.4.4; 4.4.6; 7.1.3; 7.1.4; 7.1.8].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.5; Clause 5.6; Clause 5.10** - Съпоставено с минимизиране на данните, ограничение на използването и съхранението, окончателно действие, когато вече не е необходимо, ограничение на съхранявана PII и доказателства за отчетност. Addressed by clauses [4.1.5; 4.2.1; 4.2.4; 4.3.1; 4.4.2; 4.5.1; 4.5.2; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.7; Annex A.7.2** - Съпоставено с ограничено във времето съхранение, окончателно действие, автоматизирано или ръчно прилагане и обработване на временни файлове. Addressed by clauses [4.2.3; 4.3.1; 4.4.5; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.6 ISO/IEC 27555:2025

13.6.1 **Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8** - Съпоставено с управление на рамката за изтриване, групиране на PII, срокове за съхранение и изтриване, разграничаване на архиви и резервни копия, структура на правилата за изтриване и изисквания за документирани процедури. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 7.1.1; 7.1.2].

13.6.2 **Clause 7.2; Clause 7.3; Clause 8.3** - Съпоставено с определяне на редовни срокове за изтриване, идентифициране на стандартен срок за изтриване и разпределяне на правила за изтриване към дейности по обработване на PII. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 7.1.1; 7.1.2].

13.6.3 **Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7** - Съпоставено с изисквания за внедряване за системи, ръчни процеси, аспекти на цялата организация, обработващи лични данни, обработване при възстановяване и управление на изключения. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 9.1.1; 9.1.5; 9.1.6].

13.6.4 **Clause 10.1; Clause 10.2; Clause 10.3** - Съпоставено с възлагане на роли, документация, оперативно интегриране, одит и управление на внедряването за съхранение, изтриване и унищожаване. Addressed by clauses [5.1.2; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.9; 6.1.7; 7.1.3; 7.1.4; 11.1.1; 11.1.2].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Съпоставено с основано на риска управление на поверителността, осведоменост на ръководството, интегриране на риска за поверителността в PIMS и рисковия контекст, свързан със съхранението. Addressed by clauses [4.1.6; 4.2.5; 4.5.4; 6.1.2; 6.1.3; 9.1.3; 9.1.4].

13.8 ISO/IEC 27002:2022

13.8.1 Control 7.14; Control 8.10 - Съпоставено с изтриване на информация, контролирано завършване на жизнения цикъл, освобождаване на носители за съхранение и доказателства за окончателно действие. Addressed by clauses [4.3.1; 4.3.5; 4.3.6; 4.3.7; 4.4.4; 4.4.5; 7.1.3; 7.1.4; 10.1.2].