					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII17					Заглавие на документа: **Политика за управление на документираната информация и доказателствата в PIMS**							
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	Тип покритие	Коментар
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Документирана информация за SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Документирана информация в PIMS
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Контрол на оперативните доказателства
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Доказателства за мониторинг
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Доказателства за одит
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Доказателства от преглед от ръководството
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Доказателства за несъответствия и коригиращо действие
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Записи за обработване от администратор
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Доказателства за споразумения и инструкции на обработващ лични данни
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Защита на записите
GDPR	Article 5(2)	Controller	Supporting	Доказателства за отчетност
GDPR	Article 24	Controller	Supporting	Мерки и доказателства на администратора
GDPR	Article 28	Both	Supporting	Документация на обработващия лични данни
GDPR	Article 30	Both	Supporting	Записи за обработването

GDPR	Article 32	Both	Supporting	Защита на доказателствата
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Доказателства за съответствие в областта на поверителността
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Защита на записите
ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Контрол на документираната информация
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Защита на записите
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Защита на поверителността и PII

1. Обхват

1.1 Тази политика определя задължителните изисквания за създаване, одобряване, управление на версии, защита, съхранение, извличане, превеждане, оттегляне и доказване на документираната информация в PIMS.

1.2 Тази политика се прилага за политики на PIMS, регистри, документирани одобрения, доказателствени записи, доказателства за одит, записи от прегледи от ръководството, доказателства за коригиращи действия и контролирани преводи, използвани за доказване на съответствието на PIMS.

1.3 Тази политика се прилага в контексти на администратор, съвместен администратор, обработващ лични данни и подизпълнител по обработване.

1.4 Тази политика не създава отделен регистър за контрол на документи. Доказателствата за контрол на документираната информация се поддържат чрез каноничните доказателствени обекти REG01 до REG12, като REG03 и REG12 се използват за доказателства относно приложимост на контроли, одит, несъответствия, коригиращи действия и подобрения.

2. Цел

2.1 Целта на тази политика е да гарантира, че документираната информация в PIMS е точна, контролирана, достъпна за упълномощени потребители, защитена срещу неразрешена промяна или разкриване, съхранявана за целите на одитируемостта и оттегляна, когато е остаряла.

2.2 Тази политика подпомага готовността за сертификация, като гарантира, че доказателствата, необходими за доказване на съответствието на PIMS, могат да бъдат намерени, проверени, извлечени и свързани с приложимите политики, контроли, дейности по обработване, рискове, одити и коригиращи действия.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 дефинира изискванията за контрол на документираната информация в PIMS;

3.1.2 поддържа целостта на доказателствата в REG01 до REG12;

3.1.3 гарантира проследимост на одобрението на политики и доказателства;

3.1.4 гарантира документиране на историята на версиите и решенията за оттегляне;

3.1.5 свързва доказателствата на PIMS с Декларация за приложимост и съпоставянията на политики;

3.1.6 контролира достъпа до документи и доказателствени записи на PIMS;

3.1.7 поддържа многоезично управление на версии на политики и доказателства;

3.1.8 позволява своевременно извличане на доказателства за одит;

3.1.9 предотвратява ненужна бюрокрация при контрола на документи;

3.1.10 запазва записи, готови за одит, за целите на сертификация, уверение за клиенти и непрекъснато подобрение.

4. Изявления на политиката

4.1 Контрол на документираната информация в PIMS

4.1.1 [All] Privacy Lead / PIMS Manager MUST поддържа индекс на документираната информация в PIMS в REG12 преди първоначалното публикуване на PIMS и на тримесечна база след това.

4.1.2 [All] Process Owner / Business Owner MUST идентифицира документираната информация, необходима за всяка притежавана дейност по обработване на PII, в REG02 преди започване на дейността по обработване и ежегодно след това.

4.1.3 [All] Privacy Lead / PIMS Manager MUST свърже приложимите политики, контроли и задължения за доказателства на PIMS с REG03 преди всяко издание на политика и в срок до 15 работни дни след всяка съществена промяна в приложимостта на контрол.

4.1.4 [All] Privacy Lead / PIMS Manager MUST присвои ниво на достъп и класификация на чувствителността на доказателствата към всяка категория документирана информация в PIMS в REG12 преди използване на категорията.

4.2 Създаване, одобряване, управление на версии и публикуване

4.2.1 [All] Privacy Lead / PIMS Manager MUST присвои идентификатор на документ, собственик, номер на версия, статус на одобрение, дата на влизане в сила и дата за преглед в REG12 преди публикуване на документирана информация в PIMS.

4.2.2 [All] Top Management MUST одобрява основните политики на PIMS и съществените промени в политики в REG12 преди публикуване.

4.2.3 [All] Privacy Lead / PIMS Manager MUST одобрява шаблони за доказателства на PIMS или вградени раздели на регистри в REG12 преди оперативна употреба.

4.2.4 [All] Privacy Lead / PIMS Manager MUST записва историята на версиите и обосновката на промените в REG12 преди издаване на актуализирана документирана информация в PIMS.

4.2.5 [All] Privacy Lead / PIMS Manager MUST записва комуникирането на одобрени промени в документираната информация на PIMS в REG11 в срок до 30 дни от публикуването.

[... 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 MUST поиска изключения от контрола на документирана информация или доказателства в REG12 преди отклонение от тази политика.

9.1.2 [All] Privacy Lead / PIMS Manager MUST оцени всяко изключение от контрола на документирана информация или доказателства в REG12 в срок до 10 работни дни от искането.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUST записва съвети в REG12 преди одобрение на всяко изключение, което включва разкриване на доказателства, съдържащи PII, несъответствие в превода, конфликт във връзка със съхранението или ограничение на доказателства за одит.

9.1.4 [All] Top Management MUST одобрява изключения от документираната информация, надхвърлящи 30 дни или засягащи сертификация, високорисково обработване или външно уверение, в REG12 преди изключението да влезе в сила.

9.1.5 [All] Privacy Lead / PIMS Manager MUST определя дата на изтичане, ненадхвърляща 90 дни, в REG12 за всяко одобрено изключение от контрола на документирана информация или доказателства.

9.1.6 [All] Privacy Lead / PIMS Manager MUST приключи или преоцени всяко изключение от контрола на документирана информация или доказателства в REG12 в срок до пет работни дни от изтичането му.

10. Прилагане на политиката

10.1.1 [All] Privacy Lead / PIMS Manager MUST записва липсваща, неточна, неконтролирана, остаряла или неизвлекаема документирана информация в PIMS като несъответствие в REG12 в срок до пет работни дни от идентифицирането.

10.1.2 [All] Privacy Lead / PIMS Manager MUST предотвратява публикуването на документирана информация в PIMS, когато в REG12 липсват изискваните доказателства за одобрение, версия, собственик или дата на влизане в сила.

10.1.3 [All] Process Owner / Business Owner MUST предотвратява подаването за одит на доказателства за обработване, когато в REG02 липсват изискваните доказателства за собственик, дата, статус или одобрение.

10.1.4 [All] System Owner / Application Owner MUST премахва неоторизиран достъп до хранилища на документирана информация в PIMS и записва премахването в REG12 в срок до един работен ден от идентифицирането.

10.1.5 [All] Internal Audit / Compliance Reviewer MUST проверява ефективността на коригиращите действия за несъответствия в документираната информация в REG12 при следващия планиран одит или в срок до 60 дни от приключването, което от двете настъпи първо.

11. Преглед и поддръжка

11.1.1 [All] Privacy Lead / PIMS Manager MUST преглежда тази политика ежегодно и в срок до 30 дни от съществена промяна в изискванията за документирана информация в PIMS.

11.1.2 [All] Privacy Lead / PIMS Manager MUST преглежда тази политика в срок до 30 дни след съществена одитна констатация, сертификационно несъответствие, промяна в платформата на хранилището или промяна в процеса за многоезично публикуване.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUST преглежда промените в тази политика със съществено значение за поверителността в REG12 преди одобрение.

11.1.4 [All] Top Management MUST одобрява съществените промени в тази политика в REG12 преди публикуване.

11.1.5 [All] Privacy Lead / PIMS Manager MUST записва комуникирането на одобрените промени в тази политика в REG11 в срок до 30 дни от публикуването.

12. Свързани политики

12.1 Тази политика се подкрепя от следните свързани политики:

12.2 PII01 - Политика за система за управление на информацията за поверителност

12.3 PII02 - Политика за роли, отговорности и отчетност във връзка с 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 PII05 - Политика за управление на съгласие и предпочитания

12.7 PII06 - Политика за управление на правата на субекти на данни

12.8 PII07 - Политика за оценка на риска за поверителността и DPIA

12.9 PII08 - Политика за поверителност още при проектиране и по подразбиране

12.10 PII09 - Политика за събиране, използване, разкриване и споделяне на PII

12.11 PII10 - Политика за съхранение, изтриване и унищожаване на PII

12.12 PII11 - Политика за точност и качество на PII

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

12.14 PII13 - Политика за международен трансфер на PII

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

12.16 PII15 - Политика за управление на инциденти и нарушения с PII

12.17 PII16 - Политика за обучение, осведоменост и компетентност във връзка с поверителността

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

13. Референтни стандарти и рамки

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Съпоставена с поддържането на Декларация за приложимост на PIMS, записи за приложимост на контроли и връзка между политики и доказателства. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Съпоставена с идентифициране на документирана информация, одобрение, управление на версии, достъп, извличане, запазване, оттегляне, връзка с преводни версии и метаданни за съхранение. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Съпоставена с доказателства за оперативно планиране и контрол за записи за обработване, шаблони за доказателства, качество на оперативните доказателства и външно предоставени доказателства. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Съпоставена с поддържане на документирани доказателства за измерване, резултатност при извличане, пропуски в доказателствата, несъответствия между преводни версии и приключване на прегледа на достъпа до хранилища. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Съпоставена с извличане на доказателства за одит, одитно извадково тестване, проследимост на доказателствата за одит и одитни констатации, свързани с контрола на документираната информация. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Съпоставена с доказателства от преглед от ръководството, разглеждане на контрола на документираната информация при преглед от ръководството и преглед от Top Management на резултатността на контрола на доказателствата. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Съпоставена с несъответствия в документираната информация, коригиращо действие, обработване на изключения, приключване и проверка на ефективността. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Съпоставена със записи за обработване от администратор, записи за отчетност, качество на доказателствата за обработване и съхранение на доказателства в подкрепа на задълженията на администратора. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Съпоставена със споразумение с обработващ лични данни, нареждане на клиента, външно предоставени доказателства и контрол на доказателствата за взаимоотношението с обработващия лични данни. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Съпоставена със защита на записите на PIMS срещу загуба, неразрешена промяна, неоторизиран достъп, неразрешено предоставяне и неправомерно унищожаване. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Съпоставена с доказателства за отчетност, проследимост на доказателствата, извличане на доказателства, записи за несъответствия и записи, готови за одит, които доказват съответствие. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Съпоставена с доказателства за управление от страна на администратора, записи за одобрение, контрол на политики, мерки за отчетност, документиран преглед и надзор от Top Management. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Съпоставена с документация за обработващи лични данни и подизпълнители по обработване, доказателства за нареждания на клиента, външно предоставени доказателства за процеси и контрол на разкриването на доказателства. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Съпоставена с доказателства за записи за обработване, изисквания за качество на доказателствата, референции към дейности по обработване и метаданни за собственик/статус на доказателства за обработване. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Съпоставена със защита на хранилища на доказателства, ограничения на достъпа, одобрения за достъп, преглед на защитата на хранилища и премахване на неоторизиран достъп. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Съпоставена с доказателства за съответствие в областта на поверителността, извличане на доказателства за одит, проследимост на доказателствата, подкрепа за независим преглед и доказателства за коригиращи действия. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Съпоставена със защита на записи, свързани с PII, запазване на записи и контроли за достъп и изтриване в хранилища на доказателства. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Съпоставена с идентифициране, одобрение, наличност, защита, управление на версии, съхранение, разпореждане и контрол на външно изисквана документирана информация. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Съпоставена със защита на записите на PIMS срещу загуба, унищожаване, фалшифициране, неоторизиран достъп, неразрешено предоставяне и неправомерно унищожаване. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Съпоставена със защита на поверителността и PII в документирана информация, хранилища на доказателства, разкриване и записи с контролиран достъп. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].