					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII06					Заглавие на документа: **Политика за управление на правата на субектите на данни**							
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 7.5; Clause 8.1	Both	Primary	Доказателства за искания за упражняване на права 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.1.3.2	Controller	Primary	Задължения към субектите на данни
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7	Controller	Primary	Възражение, достъп, поправка и изтриване
ISO/IEC 27701:2025	Annex A.1.3.8; Annex A.1.3.9	Controller	Primary	Уведомяване на трети страни и копие от обработваната PII
ISO/IEC 27701:2025	Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Обработване на искания и задължения при автоматизирано вземане на решения
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Записи на администратора за обработването
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Клиентско споразумение, подпомагане на задълженията и записи на обработващия лични данни
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Подкрепа от обработващия лични данни за задълженията към субектите на данни
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Защита на записите за

				искания за упражняване на права
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Прозрачност и отчетност
GDPR	Article 11; Article 12	Controller	Primary	Идентификация, начини за подаване на искания, срокове и управление на отговорите
GDPR	Article 15; Article 16; Article 17	Controller	Primary	Достъп, поправка и изтриване
GDPR	Article 18; Article 19; Article 20	Controller	Primary	Ограничаване, уведомяване и преносимост
GDPR	Article 21; Article 22	Controller	Primary	Възражение и автоматизирано вземане на решения
GDPR	Article 24	Controller	Supporting	Отговорност и мерки на администратора
GDPR	Article 26	Joint Controller	Supporting	Разпределяне на правата при съвместни администратори
GDPR	Article 28	Both	Primary	Съдействие от обработващия лични данни при искания за упражняване на права
GDPR	Article 30	Both	Supporting	Връзка със записите за обработване
GDPR	Article 32	Both	Supporting	Сигурно обработване на доказателства за права и разкриване на данни
GDPR	Article 39	Conditional	Supporting	Съвети и мониторинг от DPO, когато е приложимо

ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12	Both	Supporting	Прозрачност, участие на физическото лице, отчетност и съответствие
ISO/IEC 29151:2022	Annex A.10	Controller	Supporting	Участие и достъп на субекта на данни

1. Обхват

1.1 Настоящата политика определя задължителните изисквания за получаване, валидиране, оценяване, изпълнение, отказ, удължаване, закриване, мониторинг и доказване на исканията за упражняване на права от субекти на данни.

1.2 Настоящата политика се прилага за искания от субекти на данни или упълномощени представители относно достъп, поправка, изтриване, ограничаване, преносимост, възражение, автоматизирано вземане на решения, маршрутизиране на оттегляне на съгласие, жалби и свързани запитвания.

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

1.4 Задълженията на обработващия лични данни и подизпълнителя по обработване се прилагат само когато организацията подпомага администратор, клиент или обработващ лични данни нагоре по веригата съгласно документирани указания.

1.5 Настоящата политика не заменя следните свързани изисквания на политики:

1.5.1 PII03 относно инвентара на обработването и записите за правно основание;

1.5.2 PII04 относно съдържанието и публикуването на уведомления за поверителност;

1.5.3 PII05 относно изпълнението на съгласие и предпочитания;

1.5.4 PII10 относно изпълнението на съхранение, изтриване и унищожаване;

1.5.5 PII11 относно управлението на точността и качеството;

1.5.6 PII12 относно управлението на жизнения цикъл на обработващи лични данни и подизпълнители по обработване;

1.5.7 PII15 относно обработването на инциденти и нарушения.

2. Цел

2.1 Целта на настоящата политика е да гарантира, че исканията за упражняване на права от субекти на данни се обработват последователно, законосъобразно, сигурно, в определени срокове и с доказателства, подходящи за одит.

2.2 Настоящата политика гарантира, че организацията може да демонстрира отчетност за приемането на искания, проверката на самоличността, оценяването, изпълнението, отказа, удължаването, сътрудничеството с обработващи лични данни, закриването и непрекъснатото подобрение.

3. Цели

3.1 Целите на настоящата политика са да:

3.1.1 Осигури последователно приемане и проследяване на всички искания за упражняване на права от субекти на данни.

3.1.2 Проверява самоличността или правомощието на заявителя преди разкриване, поправка, изтриване, ограничаване или преносимост.

3.1.3 Оценява исканията спрямо записите за обработване, класификацията на ролята, правните задължения, договорните задължения и техническата осъществимост.

3.1.4 Изпълнява валидните искания в документираните срокове.

3.1.5 Записва доказателства за отказ, частично изпълнение, удължаване и закриване.

3.1.6 Подпомага задълженията на администратора, когато организацията действа като обработващ лични данни или подизпълнител по обработване.

3.1.7 Защитава записите за искания за упражняване на права и пакетите за отговор срещу неоторизирано разкриване или промяна.

3.1.8 Наблюдава резултатността при исканията за упражняване на права и инициира коригиращо действие, когато е необходимо.

4. Изисквания на политиката

4.1 Приемане, регистриране и класификация

4.1.1 [All] Privacy Lead / PIMS Manager MUST запише всяко искане за упражняване на права от субект на данни в REG06 в срок до два работни дни от получаването му.

4.1.2 [All] Privacy Lead / PIMS Manager MUST класифицира типа на всяко искане, канала на искането, датата на искането, референтната информация за самоличността на заявителя, назначения собственик, вътрешния краен срок, законоустановения или договорния краен срок и текущия статус в REG06 преди започване на оценяването.

4.1.3 [Controller] Privacy Lead / PIMS Manager MUST потвърди получаването или да предостави следващата изисквана комуникация до заявителя в срок до пет работни дни от приемането и да запише комуникацията в REG06.

4.1.4 [Controller] Process Owner / Business Owner MUST свърже всяко искане със съответната дейност по обработване в REG02, преди да бъдат възложени действия по изпълнение.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager MUST идентифицира страната - съвместен администратор, отговорна за обработването на искането, в REG02, REG06 или REG08 преди започване на същинското оценяване.

4.1.6 [Processor] Privacy Lead / PIMS Manager MUST запише всяко нареждане на клиента, свързано с искане за упражняване на права от субект на данни, в REG06 и REG08 преди започване на дейността по подпомагане.

4.1.7 [Subprocessor] Vendor / Procurement Owner MUST запише всяко нареждане нагоре по веригата, свързано с искане за упражняване на права от субект на данни, в REG06 или REG08 преди започване на дейността по подпомагане от подизпълнител по обработване.

4.1.8 [All] Incident Response Coordinator MUST запише ескалация в REG10 в срок до един работен ден, когато искане за упражняване на права указва възможен инцидент или нарушение, свързано с PII.

4.2 Проверка на самоличността, обхват и оценяване

4.2.1 [Controller] Privacy Lead / PIMS Manager MUST провери самоличността на заявителя или правомощието на представителя в REG06 преди разкриване на PII или извършване на искана промяна.

4.2.2 [Controller] Privacy Lead / PIMS Manager MUST изисква само минималната допълнителна информация, необходима за проверка, и да запише искането в REG06, когато самоличността или правомощието са недостатъчни.

4.2.3 [Controller] Process Owner / Business Owner MUST идентифицира съответните системи, записи, цели, категории PII, получатели и ограничения за съхранение от REG02 преди оценяване на изпълнението.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor MUST прегледа високорискови, оспорени, неясни, прекомерни, повтарящи се, отказани или частично изпълнени искания в REG06, преди решението да бъде съобщено.

4.2.5 [Controller] System Owner / Application Owner MUST провери, че предложените извлечения за отговор изключват несвързана PII и неоторизирани данни на трети страни преди освобождаване на пакета за отговор.

4.2.6 [Controller] Information Security Lead MUST прегледа метода за предоставяне на отговора в REG06 или REG12 преди разкриване на голям обем, чувствителна, специална категория или високорискова PII.

4.2.7 [Controller] Data Protection Officer / Privacy Advisor MUST прегледа исканията, свързани с автоматизирано вземане на решения или профилиране, в REG06 и REG04 преди изпълнение, отказ или ескалация.

4.2.8 [Both] Privacy Lead / PIMS Manager MUST запише резултата от оценяването, приложимия тип искане, решението, мотивите и следващото действие в REG06 преди изпълнение или отказ.

[... 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 изключение в REG12 преди отклонение от одобрените изисквания за приемане, проверка, изпълнение, отговор или закриване на искания за упражняване на права.

9.1.2 [All] Privacy Lead / PIMS Manager MUST одобри или отхвърли всяко изключение при обработване на права в REG12 преди внедряване.

9.1.3 [Controller] Data Protection Officer / Privacy Advisor MUST прегледа всяко изключение, включващо отказ, частично изпълнение, несигурност относно самоличността, чувствителна PII, автоматизирано вземане на решения, искания, свързани с деца, или високорисково обработване преди одобрение.

9.1.4 [Both] System Owner / Application Owner MUST блокира дейност по разкриване, поправка, изтриване, ограничаване или експортиране, когато изискваното изключение не е одобрено в REG12 преди действието.

9.1.5 [All] Privacy Lead / PIMS Manager MUST определи дата на изтичане, собственик и компенсиращ контрол за всяко одобрено изключение при обработване на права в REG12, преди изключението да стане активно.

10. Прилагане на политиката

10.1.1 [All] Privacy Lead / PIMS Manager MUST запише несъответствие в REG12 в срок до пет работни дни от установяване на просрочен, липсващ, непълен, непроверен или неподкрепен запис на искане за упражняване на права.

10.1.2 [Controller] System Owner / Application Owner MUST спре разкриването на отговор, докато проверките на самоличността, правомощието и пакета за отговор не бъдат записани в REG06.

10.1.3 [Both] Vendor / Procurement Owner MUST ескалира несътрудничество от обработващ лични данни, подизпълнител по обработване или трета страна в REG08 и REG12 в срок до пет работни дни от установяването му.

10.1.4 [All] Top Management MUST възложи собственост върху коригиращо действие в REG12, когато неизпълненията при искания за упражняване на права са системни, повтарящи се или релевантни за сертификацията.

10.1.5 [All] Internal Audit / Compliance Reviewer MUST провери доказателствата за закриване на коригиращи действия, свързани с права, в REG12 до определения краен срок.

10.1.6 [All] Incident Response Coordinator MUST инициира преглед в REG10 в срок до един работен ден, когато несъответствие при искане за упражняване на права указва неоторизирано разкриване, загуба, промяна, неналичност или друг подозиран инцидент, свързан с PII.

11. Преглед и поддръжка

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

11.1.2 [All] Privacy Lead / PIMS Manager MUST прегледа настоящата политика в срок до 30 дни от съществена промяна в законодателството относно искания за упражняване на права, обхвата на дейностите по обработване, инструментите за права, метода за проверка на самоличността, модела на услуги от обработващ лични данни или изискванията за сертификация по PIMS.

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

11.1.4 [All] Top Management MUST одобри съществените промени в настоящата политика в REG12 преди публикуване.

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

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 PII05 - Политика за управление на съгласие и предпочитания

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

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

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

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

12.11 PII11 - Политика за точност и качество на PII

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

12.13 PII13 - Политика за международно прехвърляне на PII

12.14 PII14 - Политика за сигурност и контрол на достъпа до PII

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

12.16 PII16 - Политика за обучение, осведоменост и компетентност в областта на поверителността

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

12.18 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 идентифицира вътрешните клаузи, които ги изпълняват или подкрепят.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Съпоставено с документирани записи за искания за упражняване на права, оперативен работен поток за искания, проверка на

самоличността, изпълнение, отговор, закриване и доказателства за подкрепа от обработващ лични данни. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.8; 4.3.10; 4.4.5; 7.1.1; 7.1.2; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Съпоставено с показатели за искания за упражняване на права, мониторинг на просрочени искания, извадково тестване при одит, записване на несъответствия, коригиращо действие и проверка на ефективността. Addressed by clauses [4.5.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 10.1.1; 10.1.3; 10.1.4; 10.1.5].

13.2.3 **Annex A.1.3.2** - Съпоставено с определяне и изпълнение на задължения към субектите на данни чрез документирани категории права, канали за приемане, проверка, оценяване, отговор и критерии за закриване. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.8; 4.4.1; 4.4.4; 6.1.1; 7.1.1].

13.2.4 **Annex A.1.3.6; Annex A.1.3.7** - Съпоставено с обработване на възражение, достъп, поправка, изтриване и ограничаване, проверка, изпълнение и обработване на оспорена точност. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.6; 4.4.6].

13.2.5 **Annex A.1.3.8; Annex A.1.3.9** - Съпоставено с уведомяване на трети страни след резултати от права и предоставяне на копия или преносими пакети за отговор. Addressed by clauses [4.3.5; 4.3.8; 4.5.5].

13.2.6 **Annex A.1.3.10; Annex A.1.3.11** - Съпоставено с документирано обработване на легитимни искания, срокове, удължавания, отказ, закриване и преглед на искания, свързани с автоматизирано вземане на решения. Addressed by clauses [4.1.2; 4.2.4; 4.2.7; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.2.7 **Annex A.1.2.9** - Съпоставено със свързване на искания за упражняване на права със записи за обработване, цели на обработването, системи, категории, получатели и ограничения за съхранение. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 7.1.3].

13.2.8 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Съпоставено с нареждания в клиентски споразумения, подкрепа от обработващ лични данни за задължения на клиента и записи на обработващия лични данни за дейности по подкрепа по права. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 7.1.7].

13.2.9 **Annex A.2.3.2** - Съпоставено със средства на обработващия лични данни за подкрепа на задълженията на администратора към субектите на данни, включително подкрепа за извличане, поправка, ограничаване, изтриване и експортиране съгласно документирано нареждане. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.1.7].

13.2.10 **Annex A.3.14** - Съпоставено със защита на записите за искания за упражняване на права, сигурно обработване на пакети за отговор, проверки при предоставяне на отговор и защита на доказателствата за закриване. Addressed by clauses [4.2.5; 4.2.6; 4.4.5; 4.4.7; 7.1.4; 7.1.5; 10.1.2].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(2)** - Съпоставено с прозрачно обработване на права, доказателства за отчетност, журнали на искания, записи на отговори, извадково тестване при одит и коригиращо действие. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.4; 4.4.5; 8.1.5; 10.1.1].

13.3.2 **Article 11; Article 12** - Съпоставено с идентификация, допълнителна информация когато е необходимо, срокове за отговор, комуникации, удължаване, отказ и закриване на искания. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.3.3 **Article 15; Article 16; Article 17** - Съпоставено с резултати от търсене за достъп, поправка, изтриване, проверка, доказателства за изпълнение и предоставяне на пакет за отговор. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.3.10].

13.3.4 **Article 18; Article 19; Article 20** - Съпоставено с ограничаване, уведомяване на съответните страни за резултати от права и предоставяне на преносимост или копие. Addressed by clauses [4.3.4; 4.3.5; 4.3.8; 4.5.5].

13.3.5 **Article 21; Article 22** - Съпоставено с оценяване на възражения и преглед на искания, свързани с автоматизирано вземане на решения или профилиране. Addressed by clauses [4.2.7; 4.3.6; 4.3.7].

13.3.6 **Article 24** - Съпоставено с мерки за управление от администратора, роли, собственост върху работния поток, преглед, изключения, коригиращо действие и управленски надзор върху обработването на права. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 9.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.7 **Article 26** - Съпоставено с идентифициране на отговорността на съвместния администратор за обработване на искания преди започване на същинското оценяване. Addressed by clauses [4.1.5; 6.1.5].

13.3.8 **Article 28** - Съпоставено със съдействие от обработващи лични данни и подизпълнители по обработване, документирани нареждания на клиента, срокове за подкрепа, забрана за директен отговор без разрешение и ескалация на несътрудничество. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.6; 6.1.6].

13.3.9 **Article 30** - Съпоставено със свързване на искания за упражняване на права със записи за обработване, дейности по обработване, системи, категории PII, получатели и записи на обработващия лични данни. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 4.5.1; 7.1.3].

13.3.10 **Article 32** - Съпоставено със сигурно обработване на искания за упражняване на права, защита при предоставяне на отговор, предотвратяване на неоторизирано разкриване и защита на доказателствата за права. Addressed by clauses [4.2.5; 4.2.6; 7.1.4; 7.1.5; 10.1.2; 10.1.6].

13.3.11 **Article 39** - Съпоставено със съвети и мониторинг от Data Protection Officer / Privacy Advisor за високорискови, оспорени, отказани, удължени и свързани с автоматизирано вземане на решения искания за упражняване на права. Addressed by clauses [4.2.4; 4.2.7; 4.3.7; 4.4.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12** - Съпоставено с прозрачност на каналите за права, участие и достъп на физическото лице, отчетност, процедури за жалби/правна защита, мониторинг на съответствието с изискванията за поверителност и доказателства за одит. Addressed by clauses [4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.8; 4.4.6; 7.1.1; 8.1.5; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.10** - Съпоставено с участие и достъп на субекта на данни, проверка на самоличността, достъп, поправка, изтриване, актуализации на статуса, подкрепа от обработващ лични данни и механизми за жалби/правна защита. Addressed by clauses [4.1.1; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.4; 4.5.1; 4.5.4; 8.1.6].

13.6 Вътрешни изисквания

13.6.1 Вътрешно изискване - Клаузите, определящи REG06 като основен обект за доказателства относно права, обучение, одобрение на нестандартен работен поток, изтичане на изключение, преглед на политиката и комуникация на промени в политиката, подкрепят последователността на внедряването, но не са пряко съпоставени с една външна клауза. Addressed by clauses [5.1.2; 6.1.7; 7.1.6; 9.1.4; 9.1.5; 11.1.2; 11.1.4; 11.1.5].