					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII01					Заглавие на документа: **Политика за система за управление на неприкосновеността на личната информация**							
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 4.1	Both	Primary	Определяне на контекста и ролята в PIMS
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Заинтересовани страни и изисквания
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	Обхват на PIMS
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	Създаване и подобряване на PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Лидерство и ангажираност
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Политика за поверителност
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Роли и правомощия
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Рискове и възможности
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Оценка на риска за поверителността
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Третиране на риска за поверителността и SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Цели за поверителност
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Планирани промени в PIMS
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Ресурси
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Компетентност
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Осведоменост
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Комуникации
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Документирана информация
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Оперативно планиране и контрол
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Оперативна оценка на риска

				за поверителността
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Оперативно третиране на риска за поверителността
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Мониторинг и оценяване
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Вътрешен одит
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Преглед от ръководството
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Непрекъснато подобрение
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Несъответствие и коригиращо действие
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Управленски записи на администратора
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Споразумение и цели на обработващия
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Връзка с политиката за сигурност на PII
GDPR	Article 5(2)	Controller	Supporting	Доказателства за отчетност
GDPR	Article 24	Controller	Supporting	Мерки и политика на администратора
GDPR	Article 26	Joint Controller	Supporting	Договорености между съвместни администратори
GDPR	Article 28	Both	Supporting	Управление на обработващи
GDPR	Article 30	Both	Supporting	Записи за обработването
GDPR	Article 32	Both	Supporting	Сигурност на обработването
GDPR	Article 35	Controller	Supporting	Управление на DPIA

ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Контроли и принципи за поверителност
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Процес и подготовка на PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	Програма и политика за защита на PII
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Интегриране на организационния риск за поверителността

1. Обхват

1.1 Тази политика установява системата за управление на неприкосновеността на личната информация на организацията за обработване на PII в контексти на администратор, съвместен администратор, обработващ и подизпълнител по обработване.

1.2 Тази политика се прилага за следното:

1.2.1 обхват, контекст, заинтересовани страни и организационни граници на PIMS;

1.2.2 определяне на ролята в PIMS за дейностите по обработване на PII;

1.2.3 политика за поверителност, цели за поверителност, оценка на риска за поверителността, третиране на риска за поверителността и Декларация за приложимост на PIMS;

1.2.4 управление на PIMS, мониторинг, вътрешен одит, преглед от ръководството, несъответствие, коригиращо действие и непрекъснато подобрение;

1.2.5 документирана информация и доказателства, необходими за доказване на съответствие на PIMS и отчетност.

1.3 За целите на тази политика съществена промяна означава всяка промяна, която засяга обхвата на PIMS, целите на обработване на PII, категориите PII, категориите субекти на данни, местата на обработване, разпределението на ролите на администратор или обработващ, системната архитектура, договореностите с доставчици или подизпълнители по обработване, профила на риска за поверителността, приложимите правни или договорни задължения или обхвата на сертификация.

2. Цел

2.1 Тази политика определя задължителните управленски изисквания за създаване, внедряване, поддържане, мониторинг и непрекъснато подобряване на PIMS.

2.2 Целта на тази политика е да гарантира, че организацията може да демонстрира отчетно, риск-базирано и основано на доказателства управление на обработването на PII във всички приложими роли в PIMS.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 определя обхвата, контекста, границите и приложимостта на ролите в PIMS;

3.1.2 възлага управленска отчетност за PIMS чрез каноничните роли в PIMS;

3.1.3 установява цели за поверителност и измерими очаквания за резултатността на PIMS;

3.1.4 поддържа Декларация за приложимост на PIMS за избрани и изключени контроли;

3.1.5 интегрира оценката на риска за поверителността, третирането на риска за поверителността и управлението на DPIA в работата на PIMS;

3.1.6 гарантира, че задълженията на администратор, съвместен администратор, обработващ и подизпълнител по обработване се идентифицират преди започване на обработването;

3.1.7 поддържа доказателства, подходящи за одит, за готовност за сертификация и непрекъснато подобрение;

3.1.8 избягва ненужни роли, регистри, формуляри и дублиращи се оперативни контроли.

4. Изявления на политиката

4.1 Създаване, контекст и обхват на PIMS

4.1.1 [Both] Top Management ТРЯБВА да одобри обхвата на PIMS в REG01 преди първоначалното внедряване на PIMS и в срок до 30 дни от всяка съществена промяна.

4.1.2 [Both] Privacy Lead / PIMS Manager ТРЯБВА да документира външните и вътрешните въпроси от контекста на поверителността в REG01 ежегодно и в срок до 30 дни от всяка съществена промяна.

4.1.3 [Both] Privacy Lead / PIMS Manager ТРЯБВА да документира съответните заинтересовани страни и техните изисквания към PIMS в REG01 ежегодно и в срок до 30 дни от всяка съществена промяна.

4.1.4 [Both] Privacy Lead / PIMS Manager ТРЯБВА да поддържа обобщение на взаимодействието между процесите на PIMS в REG01 преди всеки преглед от ръководството.

4.2 Определяне на ролята в PIMS

4.2.1 [Both] Process Owner / Business Owner ТРЯБВА да класифицира ролята на организацията в PIMS за всяка дейност по обработване на PII в REG02 преди започване на дейността по обработване.

4.2.2 [Joint Controller] Vendor / Procurement Owner ТРЯБВА да документира разпределението на отговорностите между съвместните администратори в REG08 преди започване на съвместното обработване.

4.2.3 [Processor] Vendor / Procurement Owner ТРЯБВА да документира инструкциите на клиента за обработване при дейности на обработващ в REG08 преди въвеждане на услугата.

4.2.4 [Subprocessor] Vendor / Procurement Owner ТРЯБВА да документира инструкциите на възходящия клиент и одобрените договорености за подизпълнители по обработване в REG08 преди започване на подизпълнителското обработване.

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

9. Изключения

9.1 Искане и одобряване на изключения

9.1.1 [All] Process Owner / Business Owner ТРЯБВА да документира всяко поискано изключение от тази политика в REG12 преди възникване на отклонението.

9.1.2 [Both] Privacy Lead / PIMS Manager ТРЯБВА да оцени риска за поверителността на всяко поискано изключение в REG04 преди одобрение.

9.1.3 [Both] Top Management ТРЯБВА да одобрява изключенията, които надвишават приетите прагове за риск за поверителността, в REG12 преди внедряване.

9.1.4 [Both] Privacy Lead / PIMS Manager ТРЯБВА да преглежда активните изключения от PIMS в REG12 на тримесечна база до приключването им.

9.2 Приключване на изключения

9.2.1 [All] Process Owner / Business Owner ТРЯБВА да документира доказателства за приключване на изключението в REG12 до одобрената дата на изтичане на изключението.

9.2.2 [Both] Internal Audit / Compliance Reviewer ТРЯБВА да проверява доказателствата за приключване на изтекли изключения в REG12 по време на следващия планиран вътрешен одит.

10. Прилагане на политиката

10.1 Обработване на несъответствия

10.1.1 [All] Privacy Lead / PIMS Manager ТРЯБВА да записва предполагаемите несъответствия с тази политика в REG12 в срок до пет работни дни от идентифицирането им.

10.1.2 [All] Process Owner / Business Owner ТРЯБВА да изпълнява одобрените коригиращи действия в REG12 до определения краен срок след одобрение на несъответствието.

10.1.3 [All] Top Management ТРЯБВА да преглежда нерешените съществени несъответствия в PIMS в REG12 при всеки преглед от ръководството.

10.1.4 [All] Internal Audit / Compliance Reviewer ТРЯБВА да проверява ефективността на коригиращите действия в REG12 в срок до 30 дни от докладваното приключване.

10.2 Ескалация

10.2.1 [All] Privacy Lead / PIMS Manager ТРЯБВА да ескалира просрочените съществени коригиращи действия към Top Management в REG12 в срок до пет работни дни след крайния срок.

10.2.2 [All] Top Management ТРЯБВА да записва решенията относно просрочените съществени коригиращи действия в REG12 в срок до 15 работни дни от ескалацията.

11. Преглед и поддържане

11.1 Преглед на политиката

11.1.1 [All] Privacy Lead / PIMS Manager ТРЯБВА да преглежда тази политика в REG12 ежегодно и в срок до 30 дни от всяка съществена промяна в правния, организационния, технологичния или сертификационния обхват или в обработването.

11.1.2 [All] Data Protection Officer / Privacy Advisor ТРЯБВА да предоставя документиран съвет в REG12 преди одобрение на политиката, когато настъпят промени в съществените задължения за поверителност.

11.1.3 [All] Top Management ТРЯБВА да одобрява съществените промени в тази политика в REG12 преди публикуване.

11.1.4 [All] Privacy Lead / PIMS Manager ТРЯБВА да актуализира REG01 и REG03 в срок до 15 работни дни след одобрени промени в политиката, които изменят обхвата на PIMS или приложимостта на контролите.

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

12. Свързани политики

12.1 Тази политика се поддържа от следните свързани политики:

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 PII07 - Политика за оценка на риска за поверителността и DPIA

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

12.6 PII12 - Политика за обработващи, подизпълнители по обработване и споделяне на данни

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

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

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

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

12.11 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 подпомага цитираните изисквания и идентифицира вътрешните клаузи, които ги прилагат или подпомагат.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Съпоставена с определяне на организационния контекст, въпросите от контекста на поверителността и приложимостта на ролята на администратор или обработващ за дейностите по PIMS. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Съпоставена с идентифициране на заинтересованите страни, субектите на данни, клиентите, надзорните органи, обработващите, подизпълнителите по обработване и техните съответни изисквания към PIMS. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Съпоставена с определяне, одобряване, поддържане и промяна на документирания обхват на PIMS. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Съпоставена със създаване, внедряване, поддържане и подобряване на процесите на PIMS и техните взаимодействия. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Съпоставена с одобрение от Top Management, ресурси, управленски преглед и лидерство по отношение на ефективността и подобряването на PIMS. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Съпоставена с поддържане на тази политика за поверителност като одобрена документирана информация и комуникиране на промени в политиката. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Съпоставена с възлагане и комуникиране на роли, отговорности и правомощия в PIMS. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Съпоставена с планиране на действия за рискове и възможности в PIMS чрез използване на контекст, изисквания на заинтересовани страни, цели и входни данни за подобрение. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Съпоставена с изискване за оценка на риска за поверителността преди ново или съществено променено обработване и поддържане на доказателства за риска за поверителността. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Съпоставена с третиране на риска за поверителността, избор на контроли, връзка с програмата за информационна сигурност и поддържане на Декларация за приложимост. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Съпоставена със създаване, измерване, мониторинг, комуникиране и актуализиране на целите на PIMS. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Съпоставена с планирани промени в PIMS и контрол на промените, засягащи обхвата, ролите, контролите и документираната информация. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Съпоставена с определяне и осигуряване на ресурси за създаване, работа, поддържане и подобряване на PIMS. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Съпоставена с очакванията за компетентност и доказателствата, подкрепящи отговорностите по PIMS и изпълнението на ролите. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Съпоставена с осведоменост за политиката за поверителност, принос към ефективността на PIMS и последиците от несъответствие. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Съпоставена с вътрешни и външни комуникации, релевантни за управлението на PIMS, промени в политиката и ескалация. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Съпоставена със създаване, поддържане, контрол, готовност на доказателствата и съхранение на документирана информация. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Съпоставена с планиране, внедряване и контрол на оперативните процеси на PIMS и външно предоставяните процеси. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Съпоставена с извършване на оценки на риска за поверителността през планирани интервали и когато се предлагат или настъпват съществени промени. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Съпоставена с изпълнение на планове за третиране на риска за поверителността и съхраняване на доказателства за резултатите от третирането. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Съпоставена с мониторинг, измерване, анализ, оценяване, показатели и докладване на ефективността на PIMS. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Съпоставена с планиране на вътрешен одит, извадкова проверка на доказателства, резултати от одит и независим преглед. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Съпоставена с входни данни за преглед от ръководството, преглед на резултатността, резултати от прегледа от ръководството и решения за подобрение. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Съпоставена с непрекъснато подобрение чрез преглед от ръководството, показатели, проследяване на коригиращи действия и поддържане на политиката. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Съпоставена с обработване на несъответствия, коригиращо действие, ескалация, приключване и проверка на ефективността. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Съпоставени със записи за цели на обработването от страна на администратора, връзка с правно основание, определяне на необходимостта от DPIA, разпределение на отговорностите между съвместни администратори и доказателствени записи за обработване. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Съпоставени със споразумения с клиенти на обработващия, документирани инструкции на клиента и ограничения на целите на обработващия. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Съпоставена с връзка с политиката за сигурност на PII, собственост върху базовия набор от контроли за сигурност на PII и статус на контролите за информационна сигурност в Декларацията за приложимост на PIMS. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Съпоставен с доказателства за отчетност, одобрение на политиката, класификация на ролята при обработване, приложимост на контролите, мониторинг, одит и записи за коригиращи действия. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Съпоставен с управленски мерки на администратора, одобрение на политиката, цели на PIMS, преглед на ефективността и документирани доказателства за отчетност на администратора. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Съпоставен с определяне и документиране на разпределението на отговорностите между съвместните администратори преди започване на съвместното обработване. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Съпоставен с управленски записи за обработващи и подизпълнители по обработване, инструкции на клиента за обработване и контрол на външно предоставяни процеси. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Съпоставен със записи за дейности по обработване, класификация на ролите, записи за отчетност на обработването и доказателства, съхранявани за възможност за одитиране. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Съпоставен с управление на базовия набор за сигурност на PII, собственост върху контролите за сигурност, статус на внедряването на сигурността и потвърждение на оперативния контрол. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Съпоставен с определяне на необходимостта от DPIA и оценка на риска за поверителността преди продължаване на високорисково или съществено променено обработване от администратор. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Съпоставени с идентифициране на контроли за поверителност, принципи на поверителност, информационна сигурност, съответствие в областта на поверителността, одит, доказателства и риск-базирано управление на поверителността. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Съпоставени с управление на PIA, определяне на тригер за DPIA, подготовка на PIA, критерии за риск за поверителността и документирани доказателства от оценка на риска за поверителността. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Съпоставени с изисквания към програма за защита на PII, идентифициране на изисквания за защита на PII, избор на контроли, базиран на риска за поверителността, и насока на политиката за защита на PII. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Съпоставени с организационни принципи за риск за поверителността, ангажираност на ръководството, интегриране на риска за поверителността в управлението на PIMS и разбиране на ролята на организацията при обработване на PII. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].