					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII18					Заглавие на документа: **Политика за мониторинг, одит и подобрение на 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	Вид покритие	Коментар
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Измерване на целите за поверителност
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Документирана информация за мониторинг, одит и подобрение
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Мониторинг на оперативното планиране и контрол
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Мониторинг, измерване, анализ 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.1.2.9	Controller	Supporting	Записи на администратора за обработването, използвани за одит
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Споразумение с обработващ лични данни и доказателства за съдействие при одит
GDPR	Article 5(2)	Controller	Supporting	Доказателства за отчетност
GDPR	Article 24	Controller	Supporting	Мерки на администратора и преглед на ефективността
GDPR	Article 28	Both	Supporting	Управление на одита и

				съдействието от обработващия лични данни
GDPR	Article 30	Both	Supporting	Записи за дейностите по обработване, използвани за одит
GDPR	Article 32	Both	Supporting	Тестване и оценяване на мерките за сигурност
GDPR	Article 39	Conditional	Supporting	Мониторинг и съвети относно одита от DPO, когато е приложимо
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Съответствие по поверителност, одит и независим надзор
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Преглед на защитата на PII и проверки за съответствие
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Мониторинг и оценяване на информационната сигурност
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Подкрепа за вътрешния одит на ISMS
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Подкрепа за прегледа от ръководството на ISMS
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Подкрепа за непрекъснато подобрение на ISMS
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Подкрепа за несъответствия и коригиращи действия в ISMS
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Независим преглед на

				информационната сигурност
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Преглед на съответствието с политики и стандарти
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Принципи, програма, провеждане и компетентност при одит на система за управление

1. Обхват

1.1 Тази политика определя изискванията на организацията за мониторинг, измерване, анализ, оценяване, вътрешен одит, преглед от ръководството, обработване на несъответствия, коригиращо действие и непрекъснато подобрение на PIMS.

1.2 Тази политика се прилага за следното:

1.2.1 всички процеси, контроли, политики, регистри, доказателствени обекти, системи, доставчици, обработващи лични данни, подизпълнители по обработване и договорености за споделяне на данни в обхвата на PIMS;

1.2.2 контекстите на организацията като администратор, съвместен администратор, обработващ лични данни и подизпълнител по обработване;

1.2.3 консолидирания мониторинг на резултатността на PIMS, целите за поверителност, статуса на внедряване на контролите, одитните констатации, несъответствията, коригиращите действия, действията от прегледа от ръководството и действията за подобрение;

1.2.4 доказателствата, съхранявани в REG12, и подкрепящите първични доказателства, съхранявани в REG01 до REG11.

1.3 Тази политика не заменя изискванията за оперативен мониторинг, определени в други политики на PIMS. Тя установява консолидирания цикъл за оценяване на резултатността, одит, преглед и подобрение на PIMS.

1.4 За целите на тази политика съществено несъответствие на PIMS означава неизпълнение, което съществено засяга обхвата на PIMS, целите за поверителност, отчетността при обработване на PII, третирането на риска за поверителността, правата на субектите на данни, сигурността на обработването, управлението на обработващи лични данни или подизпълнители по обработване, готовността при нарушение, целостта на документираните доказателства, обхвата на сертификацията или повтарящо се неизпълнение на същото изискване в рамките на 12-месечен период.

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

2. Цел

2.1 Целта на тази политика е да гарантира, че организацията оценява резултатността на PIMS, проверява съответствието на PIMS, идентифицира несъответствия, коригира слабости в контролите и непрекъснато подобрява PIMS въз основа на обективни доказателства.

2.2 Тази политика позволява на организацията да докаже, че дейностите по мониторинг, одит, преглед от ръководството и подобрение на PIMS са планирани, независими когато се изисква, основани на доказателства, своевременни и проследими до отговорни роли и канонични доказателствени обекти.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 определят консолидиран процес за мониторинг и измерване на PIMS;

3.1.2 гарантират, че целите за поверителност и резултатността на контролите на PIMS се измерват чрез документирани доказателства;

3.1.3 установят риск-базирана програма за вътрешен одит на PIMS;

3.1.4 запазят независимостта и обективността в одитните дейности на PIMS;

3.1.5 гарантират, че прегледът от ръководството получава пълни и актуални входни данни за резултатността на PIMS;

3.1.6 гарантират, че несъответствията се записват, оценяват, коригират и проверяват;

3.1.7 гарантират, че коригиращите действия се проследяват до приключване и се преглеждат за ефективност;

3.1.8 идентифицират повтарящи се слабости и възможности за подобрение;

3.1.9 подпомагат готовността за сертификация и отговорното управление на доказателства;

3.1.10 избягват дублирането на оперативни показатели, които вече са определени в свързани политики на PIMS.

4. Декларации на политиката

4.1 Рамка за мониторинг и измерване на PIMS

4.1.1 [Both] Privacy Lead / PIMS Manager MUST определи консолидираната програма за мониторинг на PIMS в REG12 преди първоначалната експлоатация на PIMS и ежегодно след това.

4.1.2 [Both] Privacy Lead / PIMS Manager MUST определи метода на измерване, честотата, източника на доказателства, целевата стойност и отговорната роля за всеки показател на PIMS в REG12 преди началото на цикъла на измерване.

4.1.3 [Both] Process Owner / Business Owner MUST предоставя на Privacy Lead / PIMS Manager входни данни за мониторинг на дейностите по обработване на PII от REG02 на тримесечна база.

4.1.4 [Both] Information Security Lead MUST предоставя на Privacy Lead / PIMS Manager входни данни за статуса на контролите за сигурност на PII от REG03 на тримесечна база.

4.1.5 [Both] Vendor / Procurement Owner MUST предоставя на Privacy Lead / PIMS Manager входни данни за статуса на обработващи лични данни, подизпълнители по обработване, споделяне с трети страни и уверение за доставчици от REG08 на тримесечна база.

4.1.6 [All] Incident Response Coordinator MUST предоставя на Privacy Lead / PIMS Manager входни данни за тенденции при инциденти с поверителността и нарушения от REG10 ежемесечно и в срок до 10 работни дни след приключване на съществен инцидент.

4.1.7 [Both] Privacy Lead / PIMS Manager MUST консолидира резултатите от мониторинга на PIMS в REG12 на тримесечна база.

4.2 Програма за вътрешен одит на PIMS

4.2.1 [All] Internal Audit / Compliance Reviewer MUST изготвя риск-базирана програма за вътрешен одит на PIMS в REG12 ежегодно преди първия планиран одитен цикъл на PIMS.

4.2.2 [All] Internal Audit / Compliance Reviewer MUST определи целта, критериите, обхвата, метода, основата за извадката и срока за докладване за всеки одит на PIMS в REG12 преди началото на одитната работа на място.

4.2.3 [All] Internal Audit / Compliance Reviewer MUST записва проверките за независимост на одитора и конфликт на интереси в REG12 преди всяко одитно възлагане.

4.2.4 [All] Privacy Lead / PIMS Manager MUST предоставя исканата контролирана документирана информация на PIMS и доказателства от регистрите чрез REG12 в срок до 10 работни дни от одобрено искане за одит.

4.2.5 [Both] Internal Audit / Compliance Reviewer MUST тества статуса на внедряване на приложимите контроли на PIMS спрямо REG03 по време на всеки одит на PIMS.

4.2.6 [Both] Internal Audit / Compliance Reviewer MUST записва избраната извадка от доказателства за обработване на PII в REG12 по време на всеки одит на PIMS.

4.2.7 [All] Internal Audit / Compliance Reviewer MUST записва резултатите от одита на PIMS в REG12 в срок до 15 работни дни след приключване на одита.

4.2.8 [All] Privacy Lead / PIMS Manager MUST възлага собственици на коригиращи действия за приети одитни констатации на PIMS в REG12 в срок до 10 работни дни от приемането на резултатите от одита.

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

9. Изключения

9.1 Изключения при мониторинг, одит и подобрение

9.1.1 [All] Process Owner / Business Owner MUST поиска всяко изключение от тази политика в REG12 преди настъпването на отклонението.

9.1.2 [All] Privacy Lead / PIMS Manager MUST оцени въздействието върху поверителността, сертификацията, одита и коригиращите действия за всяко поискано изключение в REG12 в срок до 10 работни дни от искането.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUST запише съвет в REG12 преди одобряването на всяко изключение, което засяга правни задължения, права на субекти на данни, ангажименти по DPIA, задължения за клиентски одит или високорисково обработване.

9.1.4 [All] Top Management MUST одобри изключения, които засягат изпълнението на одитния график, прегледа от ръководството, съществени несъответствия, обхвата на сертификацията или високорисково обработване, в REG12 преди влизането на изключението в сила.

9.1.5 [All] Privacy Lead / PIMS Manager MUST зададе дата на изтичане, която не надвишава 90 дни, в REG12 за всяко одобрено изключение при мониторинг, одит или подобрение.

9.1.6 [All] Privacy Lead / PIMS Manager MUST закрие или преоцени всяко изключение при мониторинг, одит или подобрение в REG12 в срок до пет работни дни от изтичането му.

10. Прилагане на политиката

10.1 Прилагане на изискванията за мониторинг, одит и подобрение

10.1.1 [All] Privacy Lead / PIMS Manager MUST записва пропуснат цикъл на мониторинг, пропуснат одит на PIMS, просрочен преглед от ръководството, липсващи доказателства за одит, просрочено коригиращо действие или просрочено действие за подобрение като несъответствие в REG12 в срок до пет работни дни от идентифицирането.

10.1.2 [All] Internal Audit / Compliance Reviewer MUST записва степента на сериозност на одитната констатация в REG12 преди издаването на одитния доклад.

10.1.3 [All] Top Management MUST изиска коригиращо действие за всяко съществено несъответствие на PIMS в REG12 в срок до 10 работни дни от ескалацията.

10.1.4 [All] Process Owner / Business Owner MUST предотврати въвеждането в експлоатация или подаването за външно уверение за високорисково обработване, когато изискваните доказателства за коригиращо действие липсват от REG12 преди въвеждането в експлоатация или подаването.

10.1.5 [All] Privacy Lead / PIMS Manager MUST ескалира повтарящи се пропуснати срокове за мониторинг или коригиращи действия към Top Management в REG12 в срок до пет работни дни след второто възникване в рамките на 12-месечен период.

10.1.6 [All] Internal Audit / Compliance Reviewer MUST провери приключването на действието по прилагане в REG12 при следващия планиран одит или в срок до 60 дни от докладваното приключване, което от двете настъпи по-рано.

11. Преглед и поддържане

11.1 Преглед и поддържане на политиката

11.1.1 [All] Privacy Lead / PIMS Manager MUST преглежда тази политика в REG12 ежегодно и в срок до 30 дни от съществена промяна в изискванията за мониторинг, одит, преглед от ръководството, коригиращо действие или сертификация на PIMS.

11.1.2 [All] Internal Audit / Compliance Reviewer MUST преглежда ефективността на програмата за одит на PIMS в REG12 ежегодно след последния планиран одит за оперативната година на PIMS.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUST преглежда значимите за поверителността промени в тази политика в REG12 преди одобрение.

11.1.4 [All] Top Management MUST одобри съществени промени в тази политика в REG12 преди публикуване.

11.1.5 [All] Privacy Lead / PIMS Manager MUST актуализира REG01 и REG03 в срок до 15 работни дни след одобрени промени в тази политика, които изменят обхвата на PIMS или приложимостта на контролите.

11.1.6 [All] Privacy Lead / PIMS Manager MUST запише комуникирането на одобрени 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 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 PII06 - Политика за управление на правата на субектите 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, свързани с PII

12.17 PII16 - Политика за обучение, осведоменост и компетентност по поверителност

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

13. Референтни стандарти и рамки

13.1 Тази 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 6.2** - Съпоставено с определянето, измерването, докладването и прегледа на целите на PIMS и показателите за резултатност на PIMS. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Съпоставено с поддържането на документирана информация за резултати от мониторинг, одитни програми, резултати от одит, доказателства за преглед от ръководството, несъответствия, коригиращи действия и действия за подобрение. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Съпоставено с функционирането на планирания цикъл за мониторинг, одит, коригиращи действия и подобрение на PIMS като част от оперативния контрол на PIMS. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Съпоставено с определянето на това какво се наблюдава и измерва, консолидирането на резултатите от мониторинга, оценяването на резултатността на PIMS и поддържането на доказателства за измерване. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Съпоставено с поддържането на програмата за вътрешен одит, планирането на одити, проверките за независимост на одиторите, извадковото събиране на доказателства, резултатите от одит и последващите действия по одитни констатации. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Съпоставено с планирането на прегледа от ръководството, прегледа на резултатността на PIMS, прегледа на тенденциите при одити и коригиращи действия, одобряването на резултатите и решенията за ресурси. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Съпоставено с идентифицирането, одобряването, изпълнението и проследяването на възможности за непрекъснато подобрение на пригодността, адекватността и ефективността на PIMS. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Съпоставено със записването на несъответствия, анализа на първопричините, планирането на коригиращи действия, изпълнението на коригиращи действия, проверката на ефективността, ескалацията и прилагането на изискванията. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Съпоставено със записите на администратора за обработването, използвани като източници на доказателства за мониторинг, извадки при одит и показатели за актуалност на инвентара на обработването. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Съпоставено с доказателства за споразумение с обработващ лични данни, клиентски одит, отговор за уверение и съдействие от обработващия лични данни, проследявани чрез процесите за уверение от доставчици и клиенти. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Съпоставено с доказателства за отчетност при мониторинг, одит, преглед от ръководството, коригиращи действия и непрекъснато подобрение. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Съпоставено с мерките за управление от администратора, прегледа на ефективността, прегледа от ръководството, коригиращите действия и документираните доказателства за подобрение. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Съпоставено с доказателства за обработващи лични данни, подизпълнители по обработване, клиентски одит, уверение от трети страни и съдействие от доставчици. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Съпоставено със записите за дейностите по обработване, използвани като доказателства за мониторинг, извадки при одит, пълнота на доказателствените обекти и актуалност на инвентара на обработването. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Съпоставено с мониторинга и оценяването на статуса на контролите за сигурност на PII, доказателствата за технически контроли и доказателствата за ефективност, свързани със сигурността. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Съпоставено със съвети по поверителност, наблюдения от мониторинг, подкрепа за одит и преглед на тенденциите в съответствието по поверителност от Data Protection Officer / Privacy Advisor, когато е приложимо. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Съпоставено с проверка на съответствието по поверителност, вътрешни или независими одити, вътрешни контроли, механизми за надзор и доказателства от оценка на риска за поверителността. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Съпоставено с независим преглед на свързаната с PII информационна сигурност, съответствието с политики и стандарти и технически преглед на съответствието за защита на PII. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Съпоставено с входни данни от мониторинг и оценяване на информационната сигурност, които подкрепят измерването на резултатността на PIMS и статуса на контролите за сигурност на PII. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Съпоставено с подкрепа от вътрешния одит на ISMS за планиране на одити на PIMS, одитни доказателства, резултати от одит и завършване на одитната програма. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Съпоставено с входни и изходни данни за преглед от ръководството за интегриран надзор върху резултатността на PIMS и информационната сигурност. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Съпоставено с непрекъснатото подобрение на PIMS и подкрепящата контролна среда за информационна сигурност. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Съпоставено с обработването на несъответствия, планирането на коригиращи действия, изпълнението на коригиращи действия и проверката на ефективността. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Съпоставено с независим преглед, проверки за независимост на одиторите, тестване на одитни доказателства и независима проверка на ефективността на коригиращите действия. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Съпоставено с прегледа на съответствието на политиките на PIMS и информационната сигурност, статуса на внедряване на контролите и доказателствата за съответствие със стандарти. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Съпоставено с принципите на одита, управлението на одитна програма, провеждането на одит, основаното на доказателства одитно докладване, последващите действия по одит и очакванията за компетентност на одиторите при одити на PIMS. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].