					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII02					Заглавие на документа: **Политика за роли, отговорности и отчетност в областта на поверителността**							
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 4.1	Both	Primary	Контекст на ролите в PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Лидерство и отчетност
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Роли, отговорности и правомощия в PIMS
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Компетентност за ролите
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Осведоменост за ролите
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Комуникация относно ролите
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Документирана информация за ролите
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Собственост върху оперативния контрол
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Роля за независим одит
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Преглед от ръководството на отчетността
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Несъответствие и коригиращо действие, свързани с роли
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Отговорност за договор с обработващ лични данни
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Роли и отговорности на съвместен администратор
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Записи за отчетност

ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Споразумения и инструкции на клиенти за обработващ лични данни
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Съгласуваност на целите на обработващия лични данни
GDPR	Article 5(2)	Controller	Supporting	Доказателства за отчетност
GDPR	Article 24	Controller	Supporting	Отговорност и мерки на администратора
GDPR	Article 26	Joint Controller	Supporting	Договорености между съвместни администратори
GDPR	Article 28	Both	Supporting	Управление и инструкции за обработващи лични данни
GDPR	Article 30	Both	Supporting	Записи за обработването и доказателства за отговорност
GDPR	Article 37	Conditional	Referenced	Определяне на DPO, когато е приложимо
GDPR	Article 38	Conditional	Supporting	Позиция и независимост на DPO, когато е приложимо
GDPR	Article 39	Conditional	Supporting	Задачи на DPO, когато е приложимо
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Участници и роли в рамката за поверителност
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Отчетност за съответствие в областта на поверителността
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Роли за защита на лично идентифицираща

				информация (PII) и разделение
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Роли и отговорности по информационна сигурност
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Разделение на задълженията

1. Обхват

1.1 Тази политика определя модела на ролите в PIMS, структурата на отчетност, правилата за възлагане на отговорности, правилата за съвместяване на роли, очакванията за ескалация и изискванията за доказателства за управлението на поверителността.

1.2 Тази политика се прилага за персонал, функции, системи, доставчици, обработващи лични данни, подизпълнители по обработване и взаимоотношения със съвместни администратори, които участват в или влияят върху обработването на лично идентифицираща информация (PII) в обхвата на PIMS.

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

1.4 Тази политика не създава нови организационни длъжности. Тя определя канонични роли в PIMS, които могат да бъдат възлагани на съществуващ персонал или функции, при условие че възлагането на ролята, компетентността, независимостта и изискванията за конфликт на интереси са документирани.

2. Цел

2.1 Целта на тази политика е да гарантира, че отговорностите в PIMS са ясно възложени, разбрани, комуникирани, доказани, преглеждани и подобрявани.

2.2 Тази политика позволява на организацията да демонстрира отчетност за управлението на поверителността, собствеността върху обработването на лично идентифицираща информация (PII), определянето на ролите на администратор и обработващ лични данни, разпределянето на отговорностите между съвместни администратори, обработването на инструкции към обработващ лични данни, отговорностите на доставчиците за поверителност, независимия преглед и ескалацията, основана на роли.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 определя каноничните роли в PIMS, използвани в набора от политики на PIMS;

3.1.2 гарантира, че за всяка съществена отговорност в PIMS е определена отчетна роля;

3.1.3 подкрепя отчетността на администратор, съвместен администратор, обработващ лични данни и подизпълнител по обработване;

3.1.4 допуска практическо съвместяване на роли за малки и средни организации, като същевременно контролира конфликтите на интереси;

3.1.5 запазва независимия преглед от Internal Audit / Compliance Reviewer;

3.1.6 гарантира, че възлагането на роли и промените в ролите се записват в канонични обекти за доказателства;

3.1.7 гарантира, че носителите на роли в PIMS получават подходяща комуникация и осведоменост;

3.1.8 гарантира, че пропуските, конфликтите и несъответствията, свързани с роли, се ескалират и коригират.

4. Изисквания на политиката

4.1 Модел и възлагане на роли в PIMS

4.1.1 [All] Top Management трябва да одобри каноничния модел на ролите в PIMS в REG01 преди първоначалното внедряване на PIMS и ежегодно след това.

4.1.2 [All] Privacy Lead / PIMS Manager трябва да поддържа поименни възлагания на роли в PIMS в REG01 преди внедряването на PIMS и в срок до 10 работни дни след промени в персонала или организацията.

4.1.3 [All] Privacy Lead / PIMS Manager трябва да документира обхвата на отговорностите и нивото на правомощия за всяка възложена роля в PIMS в REG01 преди възлагането да влезе в сила.

4.1.4 [All] Process Owner / Business Owner трябва да възложи отчетен собственик на дейността по обработване за всяка дейност по обработване на PII в REG02 преди началото на дейността по обработване.

4.1.5 [All] System Owner / Application Owner трябва да документира отчетния собственик на системата за всяка система, обработваща PII, в REG02 преди въвеждането на системата в експлоатация.

4.1.6 [All] Vendor / Procurement Owner трябва да документира собственика на взаимоотношението за всеки обработващ лични данни, подизпълнител по обработване, споделяне на данни с трета страна или взаимоотношение със съвместен администратор в REG08 преди въвеждане или одобрение на споразумение.

4.2 Съвместяване на роли, разделение и независимост

4.2.1 [All] Privacy Lead / PIMS Manager трябва да документира всяко съвместяване на роли в PIMS в REG01 преди съвместяването на роли да влезе в сила.

4.2.2 [All] Top Management трябва да одобри съвместявания на роли, включващи Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator или Internal Audit / Compliance Reviewer, в REG01 преди възлагане.

4.2.3 [All] Internal Audit / Compliance Reviewer трябва да документира независимостта от процеса на PIMS, който се преглежда, в REG12 преди началото на всеки одит на PIMS или преглед за съответствие.

4.2.4 [All] Privacy Lead / PIMS Manager трябва да записва компенсиращи контроли за неизбежни конфликти при разделението на задълженията в REG12 преди одобряване на съвместяване на роли.

4.2.5 [All] Data Protection Officer / Privacy Advisor трябва да записва опасения относно независимостта на ролята или опасения за конфликт на интереси в REG12 в срок до пет работни дни от установяването им.

[... 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 поиска изключение от отчетността на ролите в REG12 преди експлоатация на дейност по обработване на PII без изискваната възложена роля.

9.1.2 [All] Privacy Lead / PIMS Manager трябва да оцени въздействието и смекчаването на всяко изключение от отчетността на ролите в REG12 в срок до 10 работни дни от искането.

9.1.3 [All] Top Management трябва да одобри изключения от отчетността на ролите, които надвишават 30 дни или засягат високорисково обработване, в REG12 преди изключението да влезе в сила.

9.1.4 [All] Privacy Lead / PIMS Manager трябва да определи дата на изтичане, която не надвишава 90 дни, в REG12 за всяко одобрено изключение от отчетността на ролите преди одобрение.

9.1.5 [All] Privacy Lead / PIMS Manager трябва да закрие или преоцени всяко изключение от отчетността на ролите в REG12 в срок до пет работни дни след изтичането му.

10. Прилагане на политиката

10.1.1 [All] Privacy Lead / PIMS Manager трябва да записва липсващи, неточни или остарели възлагания на роли в PIMS като несъответствия в REG12 в срок до пет работни дни от установяването им.

10.1.2 [All] Top Management трябва да изисква коригиращо действие в REG12 в срок до 15 работни дни при повторни или продължителни пропуски в отчетността.

10.1.3 [All] Process Owner / Business Owner трябва да предотвратява въвеждането в експлоатация на ново или променено обработване на PII, когато изискваните доказателства за роли и отчетност липсват от REG02 или REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer трябва да проверява ефективността на коригиращите действия за несъответствия, свързани с отчетността на ролите, в REG12 при следващия планиран одит или в срок до 60 дни от закриването, което от двете настъпи по-рано.

11. Преглед и поддръжка

11.1.1 [All] Privacy Lead / PIMS Manager трябва да преглежда тази политика ежегодно и в срок до 30 дни след съществена промяна в модела на ролите в PIMS.

11.1.2 [All] Data Protection Officer / Privacy Advisor трябва да преглежда предложените промени в тази политика за въздействие върху ролите в областта на поверителността в REG12 преди одобрение.

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

11.1.4 [All] Privacy Lead / PIMS Manager трябва да актуализира REG01 и REG11 в срок до 15 работни дни след одобрени промени в ролите, отговорностите или изискванията за комуникация в PIMS.

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 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 управление на поверителността при обработващи лични данни, подизпълнители по обработване и трети страни

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

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

12.9 PII16 - Политика за обучение, осведоменост и компетентност относно поверителността

12.10 PII17 - Политика за документирана информация и управление на 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 подкрепя цитираните изисквания и идентифицира вътрешните клаузи, които ги изпълняват или подкрепят.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Съпоставена с определяне на контекста на ролите в PIMS, приложимостта за администратор и обработващ лични данни, собствеността върху обработването и записите за отговорност във взаимоотношенията. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Съпоставена с одобрение от Top Management, надзор върху отчетността, годишен преглед от ръководството, показатели за отчетност и коригиращи действия при пропуски в ролите. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Съпоставена с възлагане, документиране, комуникиране и поддържане на роли, отговорности и правомощия в PIMS, собственост върху системи, собственост върху обработването, собственост върху взаимоотношения с доставчици, собственост върху ескалация на инциденти и отговорност за независим преглед. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Съпоставена с доказателства за ролево-специфична компетентност и осведоменост за възложените отговорности в PIMS. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Съпоставена с осведоменост за възложените отговорности в PIMS, доказателства за потвърждение и годишно докладване на осведомеността за ролите. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Съпоставена с комуникация относно възлагането на роли, промени в ролите, ескалации и информация за предаване на роли. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Съпоставена с документирана информация за възлагане на роли в PIMS, обхвати на отговорностите, нива на правомощия, годишно съхранение на доказателства и поддръжка на матрицата на ролите. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Съпоставена със собственост върху оперативния контрол за дейности по обработване, системи, доставчици, обработващи лични данни, подизпълнители по обработване, взаимоотношения със съвместни администратори и контроли при въвеждане в експлоатация. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Съпоставена с независим одит и преглед за съответствие на доказателства за възлагане на роли, доказателства за съвместяване на роли, доказателства за независимост, констатации и приключване на коригиращи действия. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Съпоставена с преглед от ръководството на пълнотата на възлагането на роли в PIMS, конфликтите между роли, изключенията, показателите за отчетност и резултатите от прегледа на отчетността. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Съпоставена с ескалация, записване на несъответствия, коригиращо действие, закриване на изключения и проверка на ефективността за въпроси, свързани с отчетността на ролите. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Съпоставена с възлагане и документиране на отговорност за договор с обработващ лични данни и ескалация на отговорностите на трети страни преди одобряване или подновяване на договор. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Съпоставена с документиране на разпределението на отговорности между съвместни администратори и доказателства за отговорност във взаимоотношенията преди началото на обработване от съвместни администратори. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Съпоставена с поддържане на записи за отчетност относно собствеността върху обработване от администратор, класификацията на ролите и собствеността върху доказателствата. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Съпоставена с отговорност за клиентско споразумение на обработващ лични данни, собственост върху инструкциите на клиента и доказателства за взаимоотношение с обработващ лични данни. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Съпоставена със съгласуваност на целта и инструкциите на обработващия лични данни чрез собственост върху инструкциите на клиента и проверка на ролите на администратор/обработващ лични данни. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Съпоставена с доказателства за отчетност относно възлагането на роли, собствеността върху обработването, прегледите на ролите, несъответствията и одитните констатации. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Съпоставена с отговорността на администратора, отчетната собственост върху обработването, надзора от Top Management, годишния преглед и мерките за отчетност. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Съпоставена с документиране на разпределението на отговорности между съвместни администратори и доказателства за отговорност във взаимоотношенията преди началото на обработване от съвместни администратори. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Съпоставена с разпределение на отговорностите на обработващ лични данни и подизпълнител по обработване, собственост върху инструкции на клиента, отговорност за договор и пътища за ескалация с трети страни. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Съпоставена със записи за обработване, собственост върху обработването, класификация на ролите в PIMS и проверка на ролите на администратор/обработващ лични данни. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Съпоставена с документиране на ролята Data Protection Officer / Privacy Advisor, когато определянето е приложимо или е извършено доброволно. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Съпоставена с позицията, независимостта, участието и обработването на конфликти на интереси на Data Protection Officer / Privacy Advisor, когато е приложимо. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Съпоставена със съвети по поверителност, наблюдения от мониторинг, консултативен преглед и преглед на въздействието върху поверителността, свързан с роли, от Data Protection Officer / Privacy Advisor, когато е приложимо. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Съпоставена с участниците в рамката за поверителност и разпределението на роли за субекти на данни, администратори на PII, обработващи PII, трети страни и класификация на ролите в PIMS. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Съпоставена с отчетност за съответствие в областта на поверителността, доказателства за роли, преглед, одитни констатации и проверка на коригиращи действия. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Съпоставена с определяне на роли за защита на PII, документиране на роли, комуникация относно роли, координация между сигурност и поверителност и разделение на задълженията за защита на PII. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Съпоставена с определяне, разпределяне, документиране, комуникиране и поддържане на отговорности в PIMS и по информационна сигурност. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Съпоставена с разделение на задълженията, одобряване на съвместяване на роли, независим преглед, контроли за конфликти и проверка на коригиращи действия за конфликти между роли. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].