					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII05					Заглавие на документа: **Политика за управление на съгласията и предпочитанията**							
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	Документирана информация и оперативен контрол за доказателства за съгласие
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Мониторинг, несъответствие, коригиращо действие и подобрение
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Supporting	Връзка с правното основание
ISO/IEC 27701:2025	Annex A.1.2.4; Annex A.1.2.5	Controller	Primary	Определяне, получаване и записване на съгласие
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Записи на администратора за обработване
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Споразумения с обработващи, цели на клиента и записи на обработващия
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Supporting	Подкрепа от обработващия за задълженията на администратора към субектите на данни
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Защита на записите за обработване на PII
GDPR	Article 4(11)	Controller	Supporting	Критерии за съгласие
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Законосъобразност, добросъвестност, прозрачност и отчетност
GDPR	Article 6(1)(a); Article 6(4)	Controller	Primary	Съгласието като правно основание и връзка при променена цел

GDPR	Article 7	Controller	Primary	Условия за съгласие и оттегляне
GDPR	Article 8	Conditional	Supporting	Ескалация при съгласие на дете
GDPR	Article 9(2)(a)	Conditional	Supporting	Изрично съгласие за обработване на специални категории данни
GDPR	Article 24	Controller	Supporting	Отговорност и мерки на администратора
GDPR	Article 28	Both	Supporting	Връзка с нарежданията към обработващия и съдействието
GDPR	Article 30	Both	Supporting	Връзка със записите за обработване
ISO/IEC 29100:2020	Clause 5.2; Clause 5.8; Clause 5.12	Both	Supporting	Принципи за съгласие и избор, прозрачност и съответствие
ISO/IEC 29151:2022	Annex A.3	Both	Supporting	Контроли за съгласие и избор
ISO/IEC TS 27560:2023	Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4	Conditional	Supporting	Структура на запис и разписка за съгласие, когато се използват

1. Обхват

1.1 Тази политика определя задължителните изисквания за установяване кога се изисква съгласие, искане на съгласие, събиране на доказателства за съгласие, управление на предпочитания, обработване на оттегляния, поддържане на записи за съгласие и преглед на механизмите за даване на съгласие.

1.2 Тази политика се прилага за обработване на PII, когато съгласието е избрано или се изисква като правно основание, когато се изисква изрично съгласие, когато се събират предпочитания за съгласие или когато организацията управлява записи за съгласие от името на администратор.

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

1.4 Задълженията на обработващия и подизпълнителя по обработване се прилагат само когато записи за съгласие, състояния на предпочитания или указания за оттегляне се управляват по документирани нареждания на администратора или клиента.

1.5 Тази политика не прави съгласието правно основание по подразбиране за обработване на PII.

1.6 Определянето на правното основание продължава да се урежда от PII03 - Политика за инвентаризация на обработването на PII и правно основание.

2. Цел

2.1 Целта на тази политика е да гарантира, че управлението на съгласията и предпочитанията е законосъобразно, прозрачно, доказуемо, отменимо, технически приложимо и подкрепено от контролирани доказателства.

2.2 Тази политика гарантира, че съгласие се иска само когато е подходящо, че записите за съгласие са пълни и проследими, че оттеглянията се зачитат и че доказателствата за съгласие остават налични за целите на одит, запитвания и отчетност.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 Гарантира, че съгласието се използва само когато е подходящото правно основание или когато се изисква за дейността по обработване.

3.1.2 Гарантира, че исканията за съгласие са конкретни, информирани, разграничими и свързани с приложимото уведомление за поверителност.

3.1.3 Гарантира, че записите за съгласие и предпочитания се събират и поддържат в REG05.

3.1.4 Гарантира, че оттеглянията и промените в предпочитанията се изпълняват в рамките на определени оперативни срокове.

3.1.5 Гарантира, че записите за съгласие са свързани с целите на обработването в REG02 и версиите на уведомленията в REG07.

3.1.6 Гарантира, че дейностите на обработващи и подизпълнители по обработване в подкрепа на съгласието следват документирани нареждания на администратора или клиента.

3.1.7 Гарантира, че механизмите за даване на съгласие подлежат на мониторинг, преглед, коригиране и одитиране.

4. Изисквания на политиката

4.1 Приложимост на съгласието и правно основание

4.1.1 [Controller] Process Owner / Business Owner трябва да запише в REG02 дали съгласието се изисква или е избрано, преди да започне всяка нова или съществено променена дейност по обработване на PII, която се основава на съгласие.

4.1.2 [Controller] Privacy Lead / PIMS Manager трябва да провери в REG02 и REG05, че съгласието не е избрано като правно основание по подразбиране, преди да одобри нова или съществено променена дейност по обработване, основана на съгласие.

4.1.3 [Controller] Data Protection Officer / Privacy Advisor трябва да прегледа основанието за съгласие в REG04 преди стартиране, когато обработването включва специални категории PII, услуги, насочени към деца, високорисково обработване или дисбаланс между организацията и субекта на данни.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager трябва да документира страната, отговорна за получаване, записване, подновяване и зачитане на съгласие, в REG02 и REG05, преди да започне обработване от съвместни администратори.

4.1.5 [Processor] Privacy Lead / PIMS Manager трябва да запише нарежданията на клиента за събиране на съгласие, управление на предпочитания или подкрепа при оттегляне в REG08 и REG05, преди да внедри механизъм за даване на съгласие от името на администратор.

4.1.6 [Subprocessor] Vendor / Procurement Owner трябва да запише задълженията на подизпълнителя по обработване, свързани със съгласието, в REG08, преди на подизпълнителя по обработване да бъде разрешено да обработва записи за съгласие, състояния на предпочитания или указания за оттегляне.

4.2 Искане и събиране на съгласие

4.2.1 [Controller] Process Owner / Business Owner трябва да гарантира, че всяко искане за съгласие е специфично за целта и е свързано с приложимата версия на уведомлението за поверителност в REG07, преди искането за съгласие да бъде представено на субект на данни.

4.2.2 [Controller] System Owner / Application Owner трябва да конфигурира механизмите за даване на съгласие така, че да изискват утвърдително действие преди започване на обработването, когато се изисква изрично съгласие или съгласие чрез включване.

4.2.3 [Controller] Process Owner / Business Owner трябва да запише референцията към субекта на данни, целта, категорията PII, текста или версията на съгласието, версията на уведомлението за поверителност, канала на събиране, времевия маркер, метода, статуса и приложимия срок на валидност в REG05 при събиране на съгласие.

4.2.4 [Conditional] Privacy Lead / PIMS Manager трябва да запише логиката за установяване на възраст или разрешение в REG05 и да задейства преглед по REG04 преди стартиране, когато съгласието се отнася до обработване, насочено към деца.

4.2.5 [Conditional] Privacy Lead / PIMS Manager трябва да маркира съгласието като изрично в REG05, преди да започне обработването, когато за избраната цел се изисква изрично съгласие.

4.2.6 [Both] System Owner / Application Owner трябва да предотврати продължаването на обработване, което се основава на съгласие, преди REG05 да показва активен статус на съгласието за съответната цел.

[... 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 в REG12, преди да се отклони от одобрено изискване за събиране на съгласие, управление на предпочитания, оттегляне или доказателства.

9.1.2 [All] Privacy Lead / PIMS Manager трябва да одобри или отхвърли всяко изключение, свързано със съгласие, в REG12 преди внедряване и да определи дата на изтичане и компенсиращ контрол за всяко одобрено изключение.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor трябва да прегледа изключението в REG04 или REG12 преди одобрение, когато изключението включва изрично съгласие, обработване, насочено към деца, високорисково обработване или механизъм за оттегляне.

9.1.4 [Both] System Owner / Application Owner трябва да блокира пускането в продукционна среда или да деактивира засегнатия механизъм за даване на съгласие, когато изключение, изисквано от тази политика, не е било одобрено в REG12 преди въвеждане в експлоатация.

10. Прилагане на политиката

10.1.1 [All] Privacy Lead / PIMS Manager трябва да запише несъответствие, свързано със съгласие, в REG12 в срок до пет работни дни от установяване на липсващи, невалидни, несвързани или ненадеждни доказателства за съгласие.

10.1.2 [Controller] Process Owner / Business Owner трябва да спре или отстрани обработването за засегнатата цел, преди да продължи по-нататъшно обработване, основано на съгласие, когато съгласието се изисква, но не може да бъде доказано в REG05.

10.1.3 [Both] System Owner / Application Owner трябва да деактивира или коригира несъответстващ механизъм за събиране на съгласие, предпочитания или оттегляне в срока, определен в REG12.

10.1.4 [Processor] Vendor / Procurement Owner трябва да ескалира неизпълнения на нареждания на клиента, включващи записи за съгласие, състояния на предпочитания или подкрепа при оттегляне, в REG08 и REG12 в срок до пет работни дни от установяването им.

10.1.5 [All] Internal Audit / Compliance Reviewer трябва да провери доказателствата за приключване на коригиращите действия, свързани със съгласие, в REG12 до определения краен срок.

11. Преглед и поддръжка

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

11.1.2 [All] Privacy Lead / PIMS Manager трябва да прегледа тази политика в срок до 30 дни от съществена промяна в законодателството относно съгласието, технологиите за съгласие, инструментите за управление на предпочитания, структурата на уведомленията за поверителност или изискванията за PIMS сертификация.

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

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

11.1.5 [All] Privacy Lead / PIMS Manager трябва да записва комуникирането на одобрените промени в политиката 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 във връзка с поверителността

12.4 PII03 - Политика за инвентаризация на обработването на PII и правно основание

12.5 PII04 - Политика за уведомления за поверителност и прозрачност

12.6 PII06 - Политика за управление на правата на субектите на данни

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, подизпълнители по обработване и трети страни

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

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

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

12.16 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 прилагат или подкрепят.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Съпоставено с документирана информация и оперативен контрол за определяне на приложимостта на съгласието, събиране на доказателства за съгласие, управление на оттегляне, версииране на записи за съгласие, тестване на механизми и поддържане на REG05. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.2; 4.5.3; 4.5.4; 7.1.1; 7.1.2; 7.1.3; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Съпоставено с мониторинг на съгласието, показатели, извадкова одитна проверка, записване на несъответствия, коригиращо действие и проверка на ефективността. Addressed by clauses [4.5.5; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.2; 10.1.3; 10.1.4; 10.1.5].

13.2.3 **Annex A.1.2.3** - Съпоставено с потвърждаване кога съгласието е подходящо правно основание и със свързване на записите за съгласие със записите за правно основание в REG02. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.2; 4.5.3].

13.2.4 **Annex A.1.2.4; Annex A.1.2.5** - Съпоставено с определяне кога и как се получава съгласие, събиране на съгласие, записване на доказателство, управление на изрично съгласие, оттегляне, подновяване и статус на съгласието. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.2.5 **Annex A.1.2.9** - Съпоставено със записи на администратора за обработване, основано на съгласие, история на съгласието, връзка с уведомление, съхранение на доказателства и записи за съгласие, готови за одит. Addressed by clauses [4.2.3; 4.3.6; 4.5.1; 4.5.3; 7.1.1; 8.1.1; 8.1.3].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Съпоставено със споразуменията на обработващия с клиенти, съгласуването с целите и нарежданията на клиента и записите на обработващия, когато се предоставят услуги в подкрепа на съгласието за администратор. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 8.1.4; 10.1.4].

13.2.7 **Annex A.2.3.2** - Съпоставено с подкрепата от обработващия за задълженията на администратора към субектите на данни, когато оттегляния на съгласие, промени в предпочитания или доказателства за съгласие се обработват по нареждане на клиента. Addressed by clauses [4.3.4; 4.3.5; 4.5.4; 6.1.4; 8.1.4].

13.2.8 **Annex A.3.14** - Съпоставено със защита на записите за съгласие и предпочитания срещу неоторизирана промяна и със запазване на доказателства за одитна следа. Addressed by clauses [4.5.2; 5.1.6; 7.1.2; 10.1.5].

13.3 GDPR

13.3.1 **Article 4(11)** - Съпоставено с критерии за съгласие, които изискват съгласието да бъде конкретно, информирано, утвърдително, когато се изисква, и свързано със съответната цел и версия на уведомлението. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.5].

13.3.2 **Article 5(1)(a); Article 5(2)** - Съпоставено със законосъобразност, добросъвестност, прозрачност, доказателства за отчетност, извадкова одитна проверка, коригиращо действие и доказване на обработване, основано на съгласие. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.5.3; 4.5.5; 8.1.1; 8.1.5; 10.1.1; 10.1.5].

13.3.3 **Article 6(1)(a); Article 6(4)** - Съпоставено със съгласието като правно основание за конкретни цели и с преоценка или подновено съгласие, когато целта или условията на обработване се променят съществено. Addressed by clauses [4.1.1; 4.1.2; 4.4.1; 4.4.2; 4.5.3].

13.3.4 Article 7 - Съпоставено с доказуемост, разграничими искания за съгласие, оттегляне, лесно оттегляне, валидност на съгласието и съхранена история на съгласието. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.4; 4.4.5; 10.1.2].

13.3.5 Article 8 - Съпоставено с ескалация при съгласие за услуги, насочени към деца, логика за установяване на възраст или разрешение и преглед на риска за поверителността преди стартиране. Addressed by clauses [4.1.3; 4.2.4; 9.1.3].

13.3.6 **Article 9(2)(a)** - Съпоставено с обработване на изрично съгласие, когато изрично съгласие е избрано за обработване на специални категории данни. Addressed by clauses [4.1.3; 4.2.5; 9.1.3].

13.3.7 **Article 24** - Съпоставено с мерките за управление от администратора, преглед, одобрение, изключения, коригиращо действие и управленски надзор за контролите, свързани със съгласието. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.2; 6.1.3; 9.1.1; 9.1.2; 11.1.1; 11.1.4].

13.3.8 **Article 28** - Съпоставено с обработване на нареждания към обработващия, доказателства за подкрепа на съгласието, подкрепа при оттегляне, задължения на подизпълнителите по обработване и ескалация на нареждания на клиента. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 10.1.4].

13.3.9 **Article 30** - Съпоставено със свързване на записите за съгласие с целите на обработването, записи на администратора, записи за подкрепа от обработващия и проследимост между REG02 и REG05. Addressed by clauses [4.1.1; 4.5.3; 4.5.4; 7.1.1; 8.1.1].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.2; Clause 5.8; Clause 5.12** - Съпоставено със съгласие и избор, прозрачност и връзка с уведомление, оттегляне, отчетност и доказателства за съответствие с изискванията за поверителност. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.5.3; 4.5.5; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3** - Съпоставено с контролите за съгласие и избор, изискващи смислено, информирано и недвусмислено съгласие, промяна на предпочитания и своевременни промени в обработването след промяна или оттегляне на съгласие. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.4.5].

13.6 ISO/IEC TS 27560:2023

13.6.1 **Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4** - Съпоставено с понятията за запис и разписка за съгласие, водене на записи за съгласие, структура на запис за съгласие, статус на съгласието, връзка с версия на уведомление, структура на разписка и тълкуване на разписка за съгласие, когато такива записи или разписки се използват. Addressed by clauses [4.2.3; 4.3.2; 4.3.6; 4.4.3; 4.4.4; 4.5.2; 4.5.3; 7.1.6].

13.7 Internal Requirements

13.7.1 Internal requirement - Клаузите, които определят REG05 като официален доказателствен обект, одобрение на нестандартни доказателства, блокиране на оперативно пускане, обучение, поддръжка на политиката и комуникация, подкрепят последователността на внедряването, но не са пряко съпоставени с една външна клауза. Addressed by clauses [4.5.1; 5.1.2; 7.1.5; 9.1.4; 11.1.2; 11.1.3; 11.1.5].