| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Въведете тук наименованието на регистрираното юридическо лице | | | | | | | |
| Номер на документа:<br>PII09 | | | | | Заглавие на документа:<br>**Политика за събиране, използване, разкриване и споделяне на PII** | | | | | | | |
| Версия:<br>1.0 | | Дата на влизане в сила:<br>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 | Документиран оперативен контрол |
| ISO/IEC 27701:2025 | Clause 9.1; Clause 10.2 | Both | Supporting | Мониторинг и коригиращо действие |
| ISO/IEC 27701:2025 | Annex A.1.2.2; Annex A.1.2.9 | Controller | Primary | Цели и записи за обработването |
| ISO/IEC 27701:2025 | Annex A.1.2.3 | Controller | Referenced | Връзка с правното основание |
| ISO/IEC 27701:2025 | Annex A.1.2.8 | Joint Controller | Supporting | Отговорности при споделяне между съвместни администратори |
| ISO/IEC 27701:2025 | Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5 | Controller | Primary | Ограничения за събиране, обработване и минимизиране |
| ISO/IEC 27701:2025 | Annex A.1.5.2; Annex A.1.5.3 | Conditional | Referenced | Връзка с маршрутизирането на трансфери |
| ISO/IEC 27701:2025 | Annex A.1.5.4; Annex A.1.5.5 | Controller | Primary | Записи за трансфери и разкриване |
| ISO/IEC 27701:2025 | Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7 | Processor | Primary | Нареждания към обработващия лични данни и записи |
| ISO/IEC 27701:2025 | Annex A.2.5.2; Annex A.2.5.3 | Processor | Referenced | Връзка с маршрутизирането на трансфери от обработващ лични данни |
| ISO/IEC 27701:2025 | Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6 | Processor | Supporting | Записи и искания за разкриване от обработващ лични данни |
| GDPR | Article 5(1)(b); Article 5(1)(c); Article 5(2) | Controller | Primary | Ограничение на целите, минимизиране и отчетност |

| | | | | |
|---|---|---|---|---|
| GDPR | Article 6 | Controller | Referenced | Връзка с правното основание |
| GDPR | Article 24 | Controller | Supporting | Отговорност на администратора |
| GDPR | Article 26 | Joint Controller | Supporting | Договорености между съвместни администратори |
| GDPR | Article 28 | Both | Supporting | Нареждания към обработващия лични данни и ограничения за разкриване |
| GDPR | Article 30 | Both | Supporting | Записи за обработването и получателите |
| ISO/IEC 29100:2020 | Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6 | Both | Primary | Ограничаване на целта, събирането, минимизирането и разкриването |
| ISO/IEC 29100:2020 | Clause 5.10; Clause 5.12 | Both | Supporting | Отчетност и съответствие в областта на поверителността |
| ISO/IEC 29151:2022 | Annex A.3; Annex A.4; Annex A.5; Annex A.7 | Both | Supporting | Контроли за цел, събиране, минимизиране, използване и разкриване |

## 1. Обхват

1.1 Тази политика определя изискванията за събиране, използване, разкриване и споделяне на PII в рамките на обхвата на PIMS.

**1.2 Тази политика се прилага за:**

1.2.1 събиране на PII чрез преки, непреки, автоматизирани, ръчни, вътрешни, външни канали и канали на трети страни;

1.2.2 одобрено вътрешно използване на PII от бизнес процеси, системи и приложения;

1.2.3 вторично използване на PII за нова или съществено променена цел;

1.2.4 външно разкриване на PII пред получатели, партньори, органи, обработващи лични данни, подизпълнители по обработване, доставчици и други трети страни;

1.2.5 повтарящи се договорености за споделяне на данни и еднократни разкривания;

1.2.6 контексти на администратор, съвместен администратор, обработващ лични данни и подизпълнител по обработване;

1.2.7 REG02 - Инвентар на обработването на PII / ROPA, REG08 - Регистър на обработващите лични данни, подизпълнителите по обработване и споделянето на данни, REG09 - Регистър на международните трансфери, и REG12 - Регистър на одитите, несъответствията, коригиращите действия и подобренията.

**1.3 Тази политика не замества:**

1.3.1 PII03 относно инвентара на обработването, правното основание и собствеността върху ROPA;

1.3.2 PII04 относно съдържанието, публикуването и управлението на версиите на уведомленията за поверителност;

1.3.3 PII05 относно функционирането на съгласието и предпочитанията;

1.3.4 PII06 относно обработването на искания за упражняване на права от субекти на данни;

1.3.5 PII07 относно методологията за DPIA и оценката на риска за поверителността;

1.3.6 PII08 относно контролните точки за защита на личните данни още при проектиране;

1.3.7 PII10 относно изпълнението на съхранение, изтриване и унищожаване;

1.3.8 PII11 относно управлението на точността и качеството;

1.3.9 PII12 относно управлението на жизнения цикъл на обработващи лични данни, подизпълнители по обработване и трети страни;

1.3.10 PII13 относно избора на механизъм за международен трансфер и контролите на риска при трансфер;

1.3.11 PII14 относно сигурността на PII и контрола на достъпа;

1.3.12 PII15 относно обработването на инциденти и нарушения;

1.3.13 PII18 относно управлението на мониторинга, одита, несъответствията, коригиращите действия и подобренията в рамките на PIMS.

**1.4 За целите на тази политика:**

1.4.1 „одобрено използване“ означава използване на PII, което е записано в REG02 за конкретна дейност по обработване, цел, категория PII, категория субекти на данни, бизнес собственик и приложима PIMS роля.

1.4.2 „събиране“ означава получаване на PII директно от субект на данни, непряко от друга страна, автоматично от система или устройство, или чрез вътрешен или външен източник на данни.

1.4.3 „вторично използване“ означава използване на PII за цел, която вече не е записана като одобрена цел в REG02 за съответната дейност по обработване.

1.4.4 „проверка за съвместимост на целите“ означава документирана оценка в REG02 на първоначалната цел, предложената цел, зависимостта от правното основание, категориите PII, очакванията на субектите на данни, обосновката за минимизиране, въздействието от разкриване или трансфер и насочването към други PIMS политики, когато е необходимо.

1.4.5 „външно разкриване“ означава предоставяне на PII на страна извън организацията или извън документираната верига от нареждания на клиента.

1.4.6 „споделяне на данни“ означава повтаряща се или структурирана договореност, по силата на която PII се разкрива, прехвърля, достъпва, обменя или предоставя на друга страна.

1.4.7 „чувствително повтарящо се споделяне“ означава повтарящо се споделяне, включващо PII от специални категории, PII относно престъпления, PII на деца, записи с високо въздействие, мащабно споделяне или външно споделяне, включващо местоположение на трансфер, записано в REG09.

## 2. Цел

2.1 Целта на тази политика е да гарантира, че PII се събира, използва, разкрива и споделя само за документирани, одобрени, ограничени и отчетни цели.

2.2 Тази политика позволява на организацията да докаже, че събирането и използването са свързани със записите за обработване в REG02, че разкриванията и договореностите за споделяне на данни са записани в REG08, че маршрутизирането на международните трансфери е свързано с REG09 и че изключенията и несъответствията се обработват чрез REG12.

## 3. Цели

### 3.1 Целите на тази политика са да:

3.1.1 ограничи събирането до PII, която е необходима за документираните цели;

3.1.2 гарантира, че вътрешното използване на PII е одобрено преди започване на обработването;

3.1.3 изисква проверки за съвместимост на целите преди вторично използване;

3.1.4 изисква одобрение и доказателства преди външно разкриване;

3.1.5 поддържа доказателства за споделяне на данни в REG08, без да се създава отделен регистър за споделяне на данни;

3.1.6 насочва зависимостите при международни трансфери към REG09 и PII13, без да дублира контролите за механизми за трансфер;

3.1.7 определя периодичността на прегледите на повтарящото се споделяне;

3.1.8 поддържа доказателства, готови за одит, относно събиране, използване, разкриване, споделяне, изключения и коригиращи действия.

## 4. Изявления на политиката

### 4.1 Ограничаване на събирането

4.1.1 [Controller] Process Owner / Business Owner трябва да запише в REG02 целта на събирането, източника или канала, категориите PII, категориите субекти на данни и минималните елементи от данни, преди да започне нова дейност по събиране или съществена промяна в събирането.

4.1.2 [Controller] Privacy Lead / PIMS Manager трябва да прегледа записа за събиране в REG02 преди започване на събирането, когато се добавя нова категория PII, източник, канал или цел.

4.1.3 [Controller] Process Owner / Business Owner трябва да запише в REG02 обосновка за необходимостта на всеки елемент от PII, преди този елемент да бъде събран.

4.1.4 [Processor] Process Owner / Business Owner трябва да запише в REG02 референцията към нареждането на клиента от REG08, преди да събира PII от името на клиент.

4.1.5 [Joint Controller] Process Owner / Business Owner трябва да запише в REG08 разпределението на отговорностите за събиране между съвместните администратори, преди да започне съвместно събиране.

**4.2 Контроли за одобрено вътрешно използване**

4.2.1 [Controller] Process Owner / Business Owner трябва да запише в REG02 правилата за одобрено вътрешно използване за всяка дейност по обработване, преди използването да започне.

4.2.2 [Controller] System Owner / Application Owner трябва да внедрява само полета в работни потоци, отчети или експорти за вътрешно използване, които имат съответстващо правило за одобрено използване в REG02 преди пускане в продукционна среда.

4.2.3 [Processor] Process Owner / Business Owner трябва да запише в REG08 съответствието с нареждането на клиента, преди да използва PII на клиента за която и да е дейност като обработващ лични данни или подизпълнител по обработване.

4.2.4 [Controller] Privacy Lead / PIMS Manager трябва да преглежда правилата за одобрено използване в REG02 поне веднъж годишно за всяка активна дейност по обработване.

4.2.5 [All] Privacy Lead / PIMS Manager трябва да запише несъответствие в REG12 в срок до пет работни дни, когато бъде установено недокументирано вътрешно използване на PII.

[ ... 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 запише искане за изключение в REG12, преди да се отклони от одобрено правило за събиране, използване, разкриване или споделяне.

9.1.2 [All] Privacy Lead / PIMS Manager трябва да запише решение за одобрение или отхвърляне в REG12, преди изключението да бъде активирано.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor трябва да запише съвет в REG12 преди одобряване на изключение, включващо несъвместимо вторично използване, чувствително повтарящо се споделяне, конфликт при правно обвързващо разкриване или маршрутизиране на трансфер.

9.1.4 [All] Top Management трябва да запише одобрение в REG12 преди активиране на всяко изключение със срок над 30 календарни дни или засягащо повече от една дейност по обработване.

9.1.5 [All] Process Owner / Business Owner трябва да закрие изключение в REG12 до датата на изтичане или в срок до пет работни дни след отпадане на условието за изключението.

**10. Прилагане на политиката**

10.1.1 [All] Privacy Lead / PIMS Manager трябва да записва неодобрено събиране, използване, разкриване или споделяне като несъответствие в REG12 в срок до пет работни дни от установяването.

10.1.2 [Controller] Process Owner / Business Owner трябва да спре събирането, използването, разкриването или споделянето в срок до един работен ден, когато Privacy Lead / PIMS Manager запише в REG12 липса на одобрени доказателства в REG02 или REG08.

10.1.3 [Processor] Process Owner / Business Owner трябва да запише решение за спиране или ескалация в REG08 и REG12 в срок до един работен ден, когато PII на клиента се използва или разкрива извън документирано нареждане.

10.1.4 [All] Top Management трябва да преглежда нерешените несъответствия с високо въздействие, свързани със събиране, използване, разкриване или споделяне, в REG12 в срок до 30 календарни дни от ескалацията.

10.1.5 [All] Internal Audit / Compliance Reviewer трябва да провери доказателствата за приключване на коригиращо действие в REG12 в срок до 15 работни дни, след като Privacy Lead / PIMS Manager отбележи приключването.

## 11. Преглед и поддръжка

11.1.1 [All] Privacy Lead / PIMS Manager трябва да преглежда тази политика поне веднъж годишно и да записва решението в REG12.

11.1.2 [All] Privacy Lead / PIMS Manager трябва да прегледа тази политика в срок до 30 календарни дни от съществена промяна в обхвата на PIMS, целите на обработване, модела на споделяне, маршрутизирането на трансфери или приложимо задължение и да запише резултата в REG12.

11.1.3 [All] Process Owner / Business Owner трябва да ресертифицира активните записи в REG02 и REG08 поне веднъж годишно и в срок до 30 календарни дни от съществена промяна в обработването.

11.1.4 [All] Internal Audit / Compliance Reviewer трябва да включва контролите по PII09 в годишната одитна извадка и да записва покритието в REG12.

11.1.5 [All] Privacy Lead / PIMS Manager трябва да актуализира препратките към свързани политики в REG12 в срок до десет работни дни, когато PII03, PII08, PII10, PII12, PII13, PII14 или PII18 променя оперативната граница на тази политика.

## 12. Свързани политики

### 12.1 Тази политика следва да се чете заедно със:

12.1.1 PII01 - Политика за система за управление на неприкосновеността на личната информация

12.1.2 PII02 - Политика за роли, отговорности и отчетност в областта на поверителността

12.1.3 PII03 - Политика за инвентар на обработването на PII и правно основание

12.1.4 PII04 - Политика за уведомления за поверителност и прозрачност

12.1.5 PII05 - Политика за управление на съгласието и предпочитанията

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

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

12.1.8 PII08 - Политика за защита на личните данни още при проектиране и по подразбиране

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

12.1.10 PII11 - Политика за точност и качество на PII

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

12.1.12 PII13 - Политика за международен трансфер на PII

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

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

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

12.1.16 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 подпомага 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 документирани оперативни записи и контрол върху доказателствата за събиране, одобрено използване, вторично използване, разкриване, споделяне и маршрутизиране на трансфери. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.3; 4.3.5; 4.4.1; 4.4.2; 4.5.1; 7.1.1; 7.1.4].

13.2.2 **Clause 9.1; Clause 10.2** - Съпоставено с мониторинг, измерване, преглед, обработване на изключения, несъответствия и коригиращи действия за контролите върху събирането, използването, разкриването и споделянето. Addressed by clauses [4.2.4; 4.2.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.5; 11.1.4].

13.2.3 **Annex A.1.2.2; Annex A.1.2.9** - Съпоставено с документирани цели на администратора, записи за одобрено използване и доказателства за обработването в REG02. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.4; 4.3.1; 4.3.2; 4.3.4; 4.5.5].

13.2.4 **Annex A.1.2.3** - Съпоставено с връзката с правното основание за събиране, използване и маршрутизиране на вторично използване, без да замества PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.2.5 **Annex A.1.2.8** - Съпоставено с доказателства в REG08 за отговорностите при събиране и споделяне между съвместни администратори. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5** - Съпоставено с ограничаване на събирането, ограничаване на обработването и обосновка за минимизиране преди събиране или използване на PII. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 7.1.2].

13.2.7 **Annex A.1.5.2; Annex A.1.5.3** - Съпоставено с връзката за маршрутизиране на трансфери чрез REG09, без да замества контролите за механизми за трансфер по PII13. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.8 **Annex A.1.5.4; Annex A.1.5.5** - Съпоставено със записи за трансфери, разкривания и договорености за повтарящо се споделяне на данни в REG08. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.3; 4.5.4; 4.5.5].

13.2.9 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Съпоставено със съответствие с нарежданията на клиента към обработващия лични данни и записи на обработващия лични данни за ограниченията при събиране, използване и вторично използване. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 7.1.3; 10.1.3].

13.2.10 **Annex A.2.5.2; Annex A.2.5.3** - Съпоставено с връзката за маршрутизиране на трансфери от обработващ лични данни чрез REG09, без да замества контролите за механизми за трансфер по PII13. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.11 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Съпоставено със записи за разкриване от обработващ лични данни, статус на уведомяване при искане за разкриване и доказателства за разрешение за разкриване в REG08. Addressed by clauses [4.4.5; 4.4.6; 4.4.7; 10.1.3].

**13.3 GDPR**

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Съпоставено с ограничаване на целите, минимизиране на данните и доказателства за отчетност при събиране, използване, вторично използване, разкриване и споделяне. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3; 8.1.3; 10.1.1].

13.3.2 Article 6 - Съпоставено с връзката с правното основание и маршрутизирането при ново или несъвместимо вторично използване, без да замества PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.3.3 **Article 24** - Съпоставено с управлението от администратора, одобренията, прегледа и мерките за отчетност при събиране, използване, разкриване и споделяне. Addressed by clauses [4.1.2; 4.2.4; 4.3.2; 4.3.3; 4.3.5; 4.4.1; 6.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.4 **Article 26** - Съпоставено с доказателства за отговорностите при събиране и споделяне между съвместни администратори. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.3.5 **Article 28** - Съпоставено със съответствие с нарежданията към обработващи лични данни и подизпълнители по обработване, разрешение от клиента и ограничения за разкриване. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 4.4.5; 4.4.6; 4.4.7; 7.1.3; 10.1.3].

13.3.6 **Article 30** - Съпоставено със записи за обработване, получатели, разкриване и споделяне в REG02 и REG08. Addressed by clauses [4.1.1; 4.2.1; 4.4.2; 4.4.3; 4.5.1; 4.5.5; 8.1.1; 8.1.2].

**13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Съпоставено с определяне на целите, ограничаване на събирането, минимизиране на данните, ограничаване на използването и ограничаване на разкриването. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3].

13.4.2 **Clause 5.10; Clause 5.12** - Съпоставено с отчетност, доказателства за съответствие, преглед, управление на изключения, одитна извадка и коригиращо действие. Addressed by clauses [4.2.4; 4.2.5; 5.1.2; 6.1.1; 8.1.1; 9.1.1; 10.1.1; 11.1.4].

**13.5 ISO/IEC 29151:2022**

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Съпоставено с цел, ограничаване на събирането, минимизиране, ограничаване на използването, ограничаване на разкриването и поддръжка на записи за разкриване. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.5.3].