| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Въведете тук наименованието на регистрираното юридическо лице | | | | | | | |
| Номер на документа:<br>PII13 | | | | | Заглавие на документа:<br>**Политика за международно прехвърляне на лично идентифицираща информация (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 | Доказателства за прехвърляне и оперативен контрол |
| ISO/IEC 27701:2025 | Clause 9.1; Clause 10.2 | Both | Supporting | Мониторинг, несъответствие и коригиращо действие |
| ISO/IEC 27701:2025 | Annex A.1.2.8; Annex A.1.2.9 | Controller / Joint Controller | Supporting | Съвместна отговорност и записи за обработването |
| ISO/IEC 27701:2025 | Annex A.1.5.2; Annex A.1.5.3 | Controller | Primary | Основание за прехвърляне и местоположения на прехвърлянето |
| ISO/IEC 27701:2025 | Annex A.1.5.4; Annex A.1.5.5 | Controller | Primary | Записи за прехвърляне и разкриване |
| ISO/IEC 27701:2025 | Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7 | Processor | Supporting | Споразумение с клиента, нареждания и записи на обработващия лични данни |
| ISO/IEC 27701:2025 | Annex A.2.5.2; Annex A.2.5.3 | Processor | Primary | Основание и местоположения за прехвърляне 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 за разкриване от обработващ лични данни и правно обвързващи разкривания |
| GDPR | Article 5(2); Article 24 | Controller | Supporting | Отчетност и мерки на администратора |
| GDPR | Article 26 | Joint Controller | Supporting | Разпределение на съвместната отговорност |

| | | | | |
|---|---|---|---|---|
| GDPR | Article 28 | Processor | Supporting | Нареждания и оторизация за обработващия лични данни |
| GDPR | Article 30 | Both | Supporting | Записи за прехвърляния |
| GDPR | Article 44 | Both | Primary | Общ принцип за прехвърляне |
| GDPR | Article 45 | Controller | Primary | Механизъм за адекватност |
| GDPR | Article 46 | Controller | Primary | Подходящи гаранции |
| GDPR | Article 47 | Controller | Supporting | Обвързващи корпоративни правила |
| GDPR | Article 48 | Both | Supporting | Искания за разкриване от публични органи |
| GDPR | Article 49 | Controller | Supporting | Дерогации за специфични ситуации |
| ISO/IEC 29100:2020 | Clause 5.6; Clause 5.10; Clause 5.12 | Both | Supporting | Ограничаване на разкриването, отчетност и съответствие с изискванията за поверителност |
| ISO/IEC 29151:2022 | Annex A.7 | Both | Supporting | Защита при използване, съхранение, разкриване и прехвърляне |

## 1. Обхват

1.1 Тази политика установява изискванията на организацията за идентифициране, одобряване, записване, преглед, ограничаване и спиране на международни прехвърляния на PII.

1.2 Тази политика се прилага за дейности като администратор, съвместен администратор, обработващ лични данни и подизпълнител по обработване, при които PII се предоставя, достъпва, съхранява, хоства, разкрива или по друг начин прехвърля към държава, територия, международна организация или получател извън одобрената граница на обработване, записана в REG02 или REG09.

1.3 Тази политика се прилага за прехвърляния, включващи вътрешни свързани дружества, външни получатели, обработващи лични данни, подизпълнители по обработване, доставчици на услуги, достъп за поддръжка, хостинг местоположения, отдалечено администриране, последващи прехвърляния, искания за разкриване от публични органи и промени в услуги, свързани с прехвърляния.

1.4 Тази политика не предоставя правен съвет, не определя текст на стандартни договорни клаузи, не създава отделен регистър за оценка на въздействието на прехвърлянето, не създава отделен регистър на SCC, не определя архитектура на контролите за сигурност, не определя управление на жизнения цикъл на обработващите лични данни и не определя работен процес за реагиране при инциденти. Тези въпроси се уреждат чрез свързани политики, правна конфигурация, специфична за клиента, или одобрени доказателства в REG09.

1.5 За целите на тази политика съществена промяна в прехвърлянето означава всяка промяна в дестинацията на прехвърляне, получателя, ролята при обработване, хостинг местоположението, местоположението за достъп за поддръжка, механизма за прехвърляне, пътя на последващо прехвърляне, договорността с обработващ лични данни или подизпълнител по обработване, правното или регулаторното условие за прехвърляне, гаранцията за прехвърляне или остатъчния риск при прехвърлянето.

## 2. Цел

2.1 Целта на тази политика е да гарантира, че международните прехвърляния на PII се идентифицират преди извършването им, подкрепени са с одобрени доказателства за механизъм за прехвърляне, преглеждат се за риск при прехвърлянето, управляват се по отношение на последващите прехвърляния и се спират или отстраняват, когато изискваните доказателства или гаранции не се поддържат.

2.2 Тази политика дава възможност на организацията да демонстрира отчетно управление на прехвърлянията, като използва REG09 като основен обект с доказателства за прехвърляне, а REG02, REG08 и REG12 като поддържащи обекти с доказателства.

## 3. Цели

### 3.1 Целите на тази политика са да:

3.1.1 идентифицира международните прехвърляния на PII преди започване или промяна на обработването;

3.1.2 поддържа одобрени записи за прехвърляния в REG09;

3.1.3 документира механизмите за прехвърляне и поддържащите доказателства;

3.1.4 определя изискванията за преглед и одобрение на риска при прехвърляне;

3.1.5 контролира оторизацията на обработващи лични данни, подизпълнители по обработване и последващи прехвърляния;

3.1.6 преглежда активните прехвърляния по определена периодичност;

3.1.7 спира или отстранява прехвърляния, когато изискваните доказателства, оторизация или гаранции не се поддържат;

3.1.8 избягва ненужен текст с правни съвети, дублиращи се регистри и дублиращи се контроли за управление на доставчици.

## 4. Изявления на политиката

### 4.1 Идентифициране и регистрация на прехвърляния

4.1.1 [Controller] Process Owner / Business Owner трябва да идентифицира дестинациите за международно прехвърляне на PII, категориите получатели и местоположенията за достъп в REG02 преди дейността по обработване да започне или да бъде съществено променена.

4.1.2 [Controller] Privacy Lead / PIMS Manager трябва да създаде или актуализира записа за прехвърляне в REG09 преди започване на всяко ново или съществено променено международно прехвърляне на PII от администратор.

4.1.3 [Processor] Vendor / Procurement Owner трябва да запише оторизираните от клиента дестинации за прехвърляне от обработващ лични данни, местоположения на услуги и местоположения за отдалечен достъп в REG08 и REG09 преди дейността по прехвърляне от обработващ лични данни да започне или да бъде променена.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager трябва да запише разпределението на отговорностите между съвместните администратори за решения относно международни прехвърляния в REG08 и REG09 преди съвместната дейност по прехвърляне да започне или да бъде променена.

4.1.5 [Both] Process Owner / Business Owner трябва да идентифицира маршрутите за последващо прехвърляне, категориите последващи получатели и условията за последващо прехвърляне в REG09 преди последващото прехвърляне да бъде одобрено.

### 4.2 Избор и одобрение на механизъм за прехвърляне

4.2.1 [Controller] Privacy Lead / PIMS Manager трябва да запише одобрения механизъм за прехвърляне и поддържащите доказателства в REG09 преди започване на международно прехвърляне на PII от администратор.

4.2.2 [Controller] Data Protection Officer / Privacy Advisor трябва да прегледа доказателствата за механизма за прехвърляне в REG09 преди одобрение на ново, съществено променено или по-високорисково международно прехвърляне на PII.

4.2.3 [Processor] Vendor / Procurement Owner трябва да получи документирана оторизация или нареждане от клиента в REG08 и REG09 преди започване на всяко международно прехвърляне на PII от обработващ лични данни.

4.2.4 [Subprocessor] Vendor / Procurement Owner трябва да запише оторизацията за прехвърляне от подизпълнител по обработване и приложимите условия за прехвърляне надолу по веригата в REG08 и REG09 преди дейността по прехвърляне от подизпълнител по обработване да започне.

4.2.5 [Both] Privacy Lead / PIMS Manager трябва да блокира или отложи международно прехвърляне на PII в REG09, когато механизмът за прехвърляне, дестинацията, получателят, разпределението на ролите или поддържащите доказателства са непълни преди планираното начало на прехвърлянето.

[ ... 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 подаде всяко искане за продължаване с непълни, забавени или извънредни доказателства за прехвърляне в REG12 преди изключението да стане активно.

9.1.2 [All] Privacy Lead / PIMS Manager трябва да одобри или отхвърли исканията за изключение, свързано с прехвърляне, в REG12 преди изключението да стане активно.

9.1.3 [All] Data Protection Officer / Privacy Advisor трябва да запише становище в REG12 преди одобрение на всяко изключение, свързано с прехвърляне, което включва по-високорисково обработване, липсващи доказателства за механизъм за прехвърляне, разкриване пред публичен орган, последващо прехвърляне или въздействие върху сертификацията.

9.1.4 [All] Top Management трябва да одобри в REG12 изключенията, свързани с прехвърляния, които надхвърлят 90 дни, засягат по-високорисково обработване, засягат повтаряща се дейност по прехвърляне или засягат външно уверение, преди изключението да стане активно.

9.1.5 [All] Privacy Lead / PIMS Manager трябва да определи собственик, дата на изтичане, компенсиращ контрол и честота на преглед в REG12 за всяко одобрено изключение, свързано с прехвърляне.

9.1.6 [All] Privacy Lead / PIMS Manager трябва да преглежда всяко отворено изключение, свързано с прехвърляне, в REG12 най-малко ежемесечно до приключването му.

## 10. Прилагане на политиката

10.1.1 [All] Privacy Lead / PIMS Manager трябва да запише несъответствие в REG12 в срок до пет работни дни от идентифициране на незаписано прехвърляне, неподкрепен механизъм за прехвърляне, липсваща оторизация за обработващ лични данни, просрочен преглед, липсващи доказателства за последващо прехвърляне или неоторизирано продължаване на прехвърляне.

10.1.2 [Controller] Privacy Lead / PIMS Manager трябва да спре международно прехвърляне на PII от администратор в REG09, когато изискваните доказателства за механизма за прехвърляне липсват преди планираното начало на прехвърлянето.

10.1.3 [Processor] Vendor / Procurement Owner трябва да спре дейността по международно прехвърляне от обработващ лични данни в REG08 и REG09, когато изискваната оторизация от клиента липсва преди дейността по прехвърляне да започне.

10.1.4 [Subprocessor] Vendor / Procurement Owner трябва да ескалира неоторизирана дейност по международно прехвърляне от подизпълнител по обработване в REG08 и REG12 в срок до пет работни дни от идентифицирането ѝ.

10.1.5 [All] Top Management трябва да възложи отговорност за коригиращо действие в REG12 в срок до 10 работни дни при повторни, продължителни, високорискови или релевантни за сертификацията нарушения, свързани с прехвърляния.

10.1.6 [All] Internal Audit / Compliance Reviewer трябва да провери ефективността на коригиращите действия за несъответствия, свързани с прехвърляния, в REG12 при следващия планиран одит или в срок до 60 дни от приключването, което от двете настъпи първо.

## 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 правото относно прехвърлянията, наличността на механизъм

за прехвърляне, модела на услуги на обработващ лични данни, хостинг местоположението, местоположението за достъп за поддръжка, договорността с подизпълнител по обработване, гаранцията за прехвърляне или изискванията за PIMS сертификация.

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

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

11.1.5 [All] Privacy Lead / PIMS Manager трябва да запише 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 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 PII07 - Политика за оценка на риска за поверителността и DPIA

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

12.8 PII09 - Политика за събиране, използване, разкриване и споделяне на PII

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

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

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

12.12 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 поддържат.

### 13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Съпоставено с документирани доказателства за прехвърляне, оперативен контрол на прехвърлянията, полета за прехвърляния в REG09, одобрения на прехвърляния, записи за внедряване на прехвърляния и съгласуване на доказателства за прехвърляния. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.5; 7.1.1; 7.1.2; 7.1.3; 7.1.5; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Съпоставено с мониторинг, показатели, преглед, спиране, несъответствие и коригиращо действие за контролите върху международните прехвърляния. Addressed by clauses [4.3.4; 4.5.1; 4.5.3; 6.1.1; 6.1.2; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.6; 10.1.1; 10.1.5; 10.1.6].

13.2.3 **Annex A.1.2.8; Annex A.1.2.9** - Съпоставено с доказателства за отговорности на съвместните администратори и записи за обработване от администратор, съдържащи информация за международни прехвърляния. Addressed by clauses [4.1.1; 4.1.4; 4.1.5; 4.5.5; 6.1.4; 7.1.5].

13.2.4 **Annex A.1.5.2; Annex A.1.5.3** - Съпоставено с основание за прехвърляне от администратор, доказателства за механизъм за прехвърляне, държави, международни организации, дестинации и доказателства за преглед на прехвърляне в REG09. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.3.1; 4.5.1].

13.2.5 **Annex A.1.5.4; Annex A.1.5.5** - Съпоставено със записи за прехвърляне и разкриване, идентифициране на маршрут за последващо прехвърляне и доказателства за извършено прехвърляне или разкриване. Addressed by clauses [4.1.5; 4.4.3; 4.4.5; 7.1.7].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Съпоставено със споразумения на обработващ лични данни с клиенти, документирани нареждания от клиенти, записи на обработващия лични данни и доказателства за оторизация за международни прехвърляния от обработващ лични данни. Addressed by clauses [4.1.3; 4.2.3; 4.2.4; 4.4.2; 6.1.5; 7.1.6; 10.1.3].

13.2.7 **Annex A.2.5.2; Annex A.2.5.3** - Съпоставено с основание за прехвърляне от обработващ лични данни, оторизирани от клиента дестинации за прехвърляне, местоположения на услуги и доказателства за местоположения на прехвърляне. Addressed by clauses [4.1.3; 4.2.3; 4.2.4; 4.5.2; 7.1.6].

13.2.8 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Съпоставено със записи за разкриване от обработващ лични данни, доказателства за обработване на искания за разкриване, маршрутизиране на искания за разкриване от публични органи и доказателства за последващо прехвърляне. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 10.1.4].

**13.3 GDPR**

13.3.1 **Article 5(2); Article 24** - Съпоставено с отчетност, управление от администратора, доказателства за прехвърляне, преглед на риска при прехвърляне, обработка на изключения и коригиращо действие. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.3.4; 4.3.5; 6.1.2; 8.1.1; 9.1.2; 9.1.3; 10.1.1; 11.1.1].

13.3.2 **Article 26** - Съпоставено с разпределение на отговорностите между съвместните администратори за международни прехвърляния. Addressed by clauses [4.1.4; 6.1.4].

13.3.3 **Article 28** - Съпоставено с оторизация за прехвърляне от обработващ лични данни и подизпълнител по обработване, нареждания от клиента, доказателства за условия надолу по веригата и спиране при липсваща оторизация. Addressed by clauses [4.1.3; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 6.1.5; 10.1.3; 10.1.4].

13.3.4 **Article 30** - Съпоставено със записи за дейности по обработване и записи за прехвърляния в REG02, REG08 и REG09. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.5; 4.5.5; 7.1.5].

13.3.5 **Article 44** - Съпоставено с общо управление на прехвърлянията, одобрение на механизъм за прехвърляне, преглед на риска при прехвърляне, спиране при липсващи доказателства и повторна оценка на прехвърлянето. Addressed by clauses [4.1.2; 4.2.1; 4.2.5; 4.3.1; 4.5.3; 4.5.4].

13.3.6 **Article 45** - Съпоставено с доказателства за механизъм за прехвърляне, основан на адекватност, преглед и одобрение в REG09. Addressed by clauses [4.2.1; 4.2.2; 4.5.1].

13.3.7 **Article 46** - Съпоставено с подходящи гаранции, доказателства за гаранции, маршрутизиране при зависимост от технически гаранции и спиране на прехвърлянето, когато гаранциите липсват или са невалидни. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.5.4].

13.3.8 **Article 47** - Съпоставено с обвързващи корпоративни правила като възможен механизъм за прехвърляне, когато са приложими и записани в REG09. Addressed by clauses [4.2.1; 4.2.2; 4.3.1].

13.3.9 **Article 48** - Съпоставено със записване на искания за разкриване от чуждестранни публични органи и становище относно поверителността преди отговор, когато това е практически възможно. Addressed by clauses [4.4.3; 4.4.4].

13.3.10 **Article 49** - Съпоставено с доказателства за извънреден механизъм за прехвърляне и одобрение на изключение, когато се използват дерогации за специфични ситуации. Addressed by clauses [4.2.1; 4.2.2; 9.1.3].

**13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 5.6; Clause 5.10; Clause 5.12** - Съпоставено с ограничаване на разкриването, отчетно управление на прехвърлянията, доказателства за съответствие на прехвърлянията, преглед и коригиращо действие. Addressed by clauses [4.1.2; 4.1.5; 4.3.5; 4.4.1; 4.5.1; 6.1.1; 8.1.1; 10.1.1].

**13.5 ISO/IEC 29151:2022**

13.5.1 **Annex A.7** - Съпоставено със защита при прехвърляне, ограничаване на разкриването, доказателства за гаранции за прехвърляне, контрол на последващо прехвърляне и спиране, когато гаранциите за прехвърляне липсват или са невалидни. Addressed by clauses [4.2.1; 4.3.2; 4.3.3; 4.4.1; 4.5.3; 7.1.4].