					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII16					Заглавие на документа: **Политика за обучение, осведоменост и компетентност относно 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	Вид покритие	Коментар
ISO/IEC 27701:2025	Clause 7.2; Clause 7.3	Both	Primary	Компетентност и осведоменост
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Комуникация и документирани доказателства
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Оперативен контрол, измерване и подобрение
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Осведоменост, образование и обучение относно обработването на PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Отчетност, управление на обработващи лични данни, сигурност и задачи на DPO
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Компетентност, осведоменост и обучение
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Насоки за осведоменост, образование и обучение
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Информационна сигурност и съответствие в областта на поверителността

1. Обхват

1.1 Тази политика определя изискванията на организацията за обучение, осведоменост и компетентност относно поверителността в рамките на системата за управление на неприкосновеността на личната информация.

1.2 Тази политика се прилага за персонал, изпълнители, временен персонал, релевантни трети страни, обработващи лични данни, подизпълнители по обработване и други заинтересовани страни, чиято работа може да засяга обработването на PII, резултатността на PIMS, правата на субектите на данни, риска за поверителността, информационната сигурност, свързана с PII, нарежданията на клиента към обработващ лични данни, инциденти с поверителността, документирана информация или доказателства за съответствие.

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

1.4 Тази политика обхваща:

1.4.1 идентифициране на целевата аудитория на обучението по поверителност;

1.4.2 въвеждащо обучение;

1.4.3 ежегодно опреснително обучение;

1.4.4 ролево базирано обучение и обучение, задействано от събитие;

1.4.5 доказателства за завършване на обучение;

1.4.6 ескалация при незавършено обучение;

1.4.7 преглед на ефективността на обучението;

1.4.8 доказателства за уверение относно обучението на обработващи лични данни, подизпълнители по обработване и трети страни.

1.5 Тази политика не създава отделна матрица за обучение, табло за обучение, регистър на човешките ресурси, регистър на компетентността, дисциплинарен регистър или регистър за обучение на клиенти. Възлаганията на обучения, завършванията, напомнянията, доказателствата за компетентност и доказателствата за осведоменост се записват в REG11, а изключенията, ескалациите, несъответствията, коригиращите действия и доказателствата от прегледи се записват в REG12. Доказателствата за уверение относно обучението на обработващи лични данни, подизпълнители по обработване и трети страни се записват в REG08, когато е приложимо.

1.6 Тази политика не дублира:

1.6.1 възлагането на отчетност по роли в PII02;

1.6.2 инвентара на обработването и изискванията за правно основание в PII03;

1.6.3 методологията за риск за поверителността и DPIA в PII07;

1.6.4 контролните точки за поверителност още при проектиране в PII08;

1.6.5 управлението на жизнения цикъл на обработващите лични данни в PII12;

1.6.6 функционирането на сигурността и контрола на достъпа за PII в PII14;

1.6.7 работния процес за инциденти с PII и нарушения на сигурността в PII15;

1.6.8 управлението на документирана информация в PII17;

1.6.9 управлението на мониторинга, вътрешния одит и подобренията в PII18.

2. Цел

2.1 Целта на тази политика е да гарантира, че лицата, чиято работа засяга обработването на PII, разбират своите отговорности относно поверителността, завършват подходящо обучение по определена периодичност, поддържат компетентност, релевантна за ролята им, и генерират одитируеми доказателства за обучение, осведоменост и ескалация.

2.2 Тази политика подпомага последователното прилагане на PIMS чрез използване на REG11 като основен доказателствен обект за обучение и осведоменост и на REG08, REG10 и REG12 като поддържащи доказателствени обекти.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 дефинира целевите аудитории за обучение по поверителност;

3.1.2 дефинира изискванията за въвеждащо обучение;

3.1.3 дефинира изискванията за ежегодно опреснително обучение;

3.1.4 дефинира изискванията за ролево базирано обучение по поверителност;

3.1.5 записва доказателствата за завършване в REG11;

3.1.6 ескалира незавършеното обучение чрез REG12;

3.1.7 поддържа доказателства за уверение относно обучението на обработващи лични данни, подизпълнители по обработване и трети страни в REG08, когато е приложимо;

3.1.8 преглежда ефективността на обучението, без да създава прекомерни показатели или дублиращи се регистри;

3.1.9 гарантира, че съдържанието на обучението остава съгласувано с текущите политики на PIMS и съществените задължения в областта на поверителността.

4. Изявления на политиката

4.1 Целева аудитория и възлагане на обучението

4.1.1 [All] Privacy Lead / PIMS Manager ТРЯБВА да дефинира категориите целева аудитория за обучение по PIMS в REG11 преди началото на всеки годишен цикъл на обучение.

4.1.2 [All] Process Owner / Business Owner ТРЯБВА да идентифицира в REG11 персонала, чиито задължения включват обработване на PII, преди въвеждане в длъжност, присвояване на роля или съществена промяна в задълженията.

4.1.3 [Conditional] System Owner / Application Owner ТРЯБВА да идентифицира в REG11 потребителите, които се нуждаят от обучение по поверителност за система за PII, привилегирован достъп или административни функции, преди достъпът да бъде активиран или съществено променен.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager ТРЯБВА да запише разпределението на отговорностите за обучение между съвместните администратори в REG11 или REG08 преди започване или съществена промяна на съвместна дейност по обработване.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor ТРЯБВА да идентифицира повишените потребности от обучение по поверителност в REG11 преди възлагане на обучение на роли, които работят с високорисково обработване, PII от специални категории, права на субекти на данни, DPIAs, международни трансфери или оценка на нарушението.

4.1.6 [All] Privacy Lead / PIMS Manager ТРЯБВА да запише възложената целева аудитория на обучението, вида обучение, изискваната дата на завършване и отговорника за доказателствата в REG11 преди началото на всеки годишен цикъл на обучение.

4.2 Периодичност на въвеждащото и ежегодното обучение

4.2.1 [All] Privacy Lead / PIMS Manager ТРЯБВА да възложи базово обучение за осведоменост относно поверителността в REG11 в срок до 10 работни дни от въвеждането в длъжност за персонал с достъп до PII или с отговорности по PIMS.

4.2.2 [All] Process Owner / Business Owner ТРЯБВА да гарантира, че назначеният персонал завършва въвеждащото обучение по поверителност в REG11 преди одобряване на достъп без надзор до PII или в срок до 30 дни от въвеждането в длъжност, което от двете настъпи по-рано.

4.2.3 [All] Privacy Lead / PIMS Manager ТРЯБВА да възлага ежегодно опреснително обучение по поверителност в REG11 най-малко веднъж на всеки 12 месеца.

4.2.4 [All] Process Owner / Business Owner ТРЯБВА да потвърди статуса на завършване на ежегодното опреснително обучение за назначения персонал в REG11 до публикувания годишен краен срок.

4.2.5 [Conditional] Privacy Lead / PIMS Manager ТРЯБВА да възложи целенасочено опреснително обучение в REG11 в срок до 30 дни след съществена промяна в политика за поверителност, съществена промяна в процес на PIMS, одитна констатация, повтарящ се неуспех при обучение или релевантен урок от инцидент с 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 от обучение по поверителност в REG12 преди удължаване на изисквания краен срок за завършване.

9.1.2 [All] Privacy Lead / PIMS Manager ТРЯБВА да одобри или отхвърли исканията за изключение от обучение по поверителност в REG12 преди изключението да стане активно.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor ТРЯБВА да даде становище относно изключенията от обучение в REG12 преди одобрение, когато изключението засяга високорисково обработване, PII от специални категории, обработване на искания за упражняване на права, обработване на инциденти, международни трансфери или доказателства за сертификация.

9.1.4 [Conditional] Top Management ТРЯБВА да одобри изключенията от обучение по поверителност в REG12 преди активиране, когато изключението засяга повтарящо се незавършване, привилегирован достъп до PII, обработване на PII с високо въздействие или доказателства, предназначени за регулаторни органи.

9.1.5 [All] Privacy Lead / PIMS Manager ТРЯБВА да дефинира отговорник за изключението, дата на изтичане, компенсиращо действие и дата за преглед в REG12 преди одобряване на каквото и да е изключение от обучение по поверителност.

9.1.6 [All] Process Owner / Business Owner ТРЯБВА да закрие или поднови одобрените изключения от обучение по поверителност в REG12 преди датата на изтичане на изключението.

10. Прилагане на политиката

10.1.1 [All] Privacy Lead / PIMS Manager ТРЯБВА да запише несъответствие в обучението в REG12 в срок до пет работни дни, когато доказателства за задължително обучение по поверителност липсват, са непълни, просрочени или не могат да бъдат проследени до REG11.

10.1.2 [All] Process Owner / Business Owner ТРЯБВА да гарантира, че просроченото задължително обучение по поверителност е завършено или ескалирано в REG11 или REG12 в срок до 10 работни дни след записване на статуса „просрочено“.

10.1.3 [Conditional] System Owner / Application Owner ТРЯБВА да ограничи нов достъп до PII с високо въздействие в REG12, когато изискването въвеждащо или ролево базирано обучение по поверителност остава незавършено след ескалация.

10.1.4 [Processor] Vendor / Procurement Owner ТРЯБВА да ескалира липсващи доказателства за уверение относно обучението на обработващ лични данни, подизпълнител по обработване или външна работна сила в REG08 и REG12 в срок до пет работни дни след идентифициране.

10.1.5 [Conditional] Incident Response Coordinator ТРЯБВА да свърже действията по прилагане, свързани с обучението, с REG10 в срок до един работен ден, когато неуспехът в обучението е допринесъл за предполагаем или потвърден инцидент с PII.

10.1.6 [All] Internal Audit / Compliance Reviewer ТРЯБВА да провери доказателствата за приключване на коригиращите действия, свързани с обучението, в REG12 при следващия планиран одит или в срок до 60 дни от приключването, което от двете настъпи по-рано.

11. Преглед и поддръжка

11.1.1 [All] Privacy Lead / PIMS Manager ТРЯБВА да преглежда тази политика и съдържанието на обучението най-малко ежегодно и да записва резултата от прегледа в REG11 или REG12.

11.1.2 [All] Privacy Lead / PIMS Manager ТРЯБВА да прегледа тази политика в срок до 30 дни след съществена промяна в обхвата на PIMS, законодателството в областта на поверителността, дейностите по обработване, модела на ролите, уроците от инциденти, одитните констатации или резултатите за ефективността на обучението.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor ТРЯБВА да прегледа промените в политиката 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 актуализира съдържанието на обучението и доказателствата за възлагане в REG11 в срок до 30 дни след одобрена съществена промяна в политиката.

12. Свързани политики

12.1 Тази политика следва да се чете заедно със:

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 съгласия и предпочитания;

12.7 PII06 - Политика за управление на правата на субекти 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 PII12 - Политика за управление на поверителността при обработващи лични данни, подизпълнители по обработване и трети страни;

12.13 PII13 - Политика за международен трансфер на PII;

12.14 PII14 - Политика за сигурност и контрол на достъпа за PII;

12.15 PII15 - Политика за управление на инциденти с PII и нарушения на сигурността;

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

12.17 PII18 - Политика за мониторинг, одит и подобрение на PIMS.

13. Референтни стандарти и рамки

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].