					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII08					Заглавие на документа: **Политика за поверителност още при проектиране и защита на личните данни по подразбиране**							
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 6.1.2; Clause 6.1.3	Both	Supporting	Връзка с оценката и третирането на риска за поверителността
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Планирани промени и оперативен контрол
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Документирани доказателства за дизайн за поверителност
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.1.2.6; Annex A.1.2.9	Controller	Supporting	Цели, критерий за задействане на PIA и записи
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Ограничаване на събирането и обработването
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Цели за точност и минимизиране
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Дизайн за деидентификация, изтриване и временни файлове
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Споразумение с клиента, поддръжка и записи на обработващия лични данни
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Възможности за дизайн на обработващия лични данни
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Жизнен цикъл на разработката и инженерни принципи
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Ограничаване на целите,

				минимизиране и отчетност
GDPR	Article 24	Controller	Supporting	Мерки на администратора
GDPR	Article 25	Controller	Primary	Защита на данните още при проектиране и по подразбиране
GDPR	Article 28	Both	Supporting	Нареждания и съдействие за обработващия лични данни
GDPR	Article 30	Both	Supporting	Записи за обработването
GDPR	Article 35	Controller	Supporting	Връзка с критерий за задействане на DPIA
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Контроли за поверителност още при проектиране
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Цел, събиране, минимизиране и ограничаване на използването
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Точност, отчетност и съответствие
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	Принципи и контроли за защита на PII

1. Обхват

1.1 Тази политика определя изискванията за вграждане на поверителност още при проектиране и защита на личните данни по подразбиране в нови и променени дейности по обработване на PII, проекти, продукти, услуги, системи, приложения, интеграции, дейности по набавяне и промени в бизнес процеси в обхвата на PIMS.

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

1.3 Задълженията на обработващия лични данни и подизпълнителя по обработване се прилагат, когато организацията проектира, конфигурира, променя или извършва обработване от името на клиент, администратор или обработващ лични данни нагоре по веригата съгласно документирани нареждания.

1.4 Тази политика обхваща следното:

1.4.1 изисквания за поверителност при започване на проект;

1.4.2 контроли за дизайн, свързани с целта, минимизирането на данните и настройките по подразбиране;

1.4.3 преглед на дизайна за поверителност преди въвеждане в експлоатация;

1.4.4 преглед на дизайна за поверителност, задействан от промяна;

1.4.5 проверки за защита на личните данни още при проектиране при набавяне;

1.4.6 връзка с риска за поверителността, проверката за необходимост от DPIA и доказателствата за коригиращо действие.

1.5 Тази политика не заменя следното:

1.5.1 PII03 за инвентара на обработването, целите, правното основание и записите по ROPA;

1.5.2 PII04 за съдържанието и публикуването на уведомление за поверителност;

1.5.3 PII05 за контролите за съгласие и предпочитания;

1.5.4 PII06 за обработването на права на субекти на данни;

1.5.5 PII07 за методологията за оценка на риска за поверителността и DPIA;

1.5.6 PII09 за контролите за събиране, използване, разкриване и споделяне;

1.5.7 PII10 за изпълнението на съхранение, изтриване и унищожаване;

1.5.8 PII11 за операциите по точност и качество;

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

1.5.10 PII13 за механизмите за международен трансфер;

1.5.11 PII14 за операциите по сигурност на PII и контрол на достъпа;

1.5.12 PII18 за управлението на мониторинга, одита, коригиращите действия и подобренията в рамките на PIMS.

2. Цел

2.1 Целта на тази политика е да гарантира, че изискванията за поверителност се идентифицират, внедряват и доказват преди обработването на PII да започне или да се промени съществено, както и че системите и процесите са конфигурирани по подразбиране така, че да ограничават събирането, използването, експонирането, зависимостта от съхранение, зависимостта от разкриване и идентифицируемостта на PII до необходимото за документираната цел.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 вгради изискванията за поверителност в решенията за започване, проектиране, набавяне, промяна и въвеждане в експлоатация на проекти;

3.1.2 гарантира, че дизайните за обработване на PII са свързани с документирани цели и записи за обработване в REG02;

3.1.3 внедри настройки по подразбиране за минимизиране на данните и защита на поверителността преди започване на обработването;

3.1.4 гарантира, че рискът за поверителността и проверката за необходимост от DPIA се задействат, без да се дублира методологията по PII07;

3.1.5 гарантира, че изискванията за набавяне и дизайн на обработващия лични данни се записват, без да се дублира управлението на жизнения цикъл по PII12;

3.1.6 гарантира, че нерешените проблеми в дизайна се ескалират чрез REG12;

3.1.7 поддържа доказателства за дизайн, готови за одит, в REG02, REG04, REG08 и REG12.

4. Изявления на политиката

4.1 Започване на проект и изисквания за поверителност

4.1.1 [Both] The Process Owner / Business Owner MUST запише запис за дизайн за поверителност в REG04 преди започване на всеки проект, продукт, услуга, система, приложение, интеграция или промяна в бизнес процес, които включват PII.

4.1.2 [Both] The Process Owner / Business Owner MUST свърже всеки запис за дизайн за поверителност в REG04 със съществуваща или проектна дейност по обработване в REG02, преди да бъдат одобрени функционалните изисквания.

4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST запише изискванията на администратора за защита на личните данни още при проектиране в REG04 преди одобрение на функционалния дизайн на администратора.

4.1.4 [Processor] The Vendor / Procurement Owner MUST запише нарежданията на клиента относно дизайна за поверителност и договорните ограничения за дизайн в REG08 преди одобрение на дизайна на услуга на обработващия лични данни или на съществена промяна в услугата.

4.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST запише становище в REG04 преди одобряване на дизайн за PII, който е високорисков, нов, чувствителен, автоматизиран, мащабен или съществено променен.

4.1.6 [Both] The Information Security Lead MUST запише зависимостите от контроли за сигурност на PII, които подпомагат дизайна за поверителност, в REG04 преди одобрение на архитектурата.

4.2 Минимизиране на данните и дизайн за поверителност по подразбиране

4.2.1 [Controller] The Process Owner / Business Owner MUST документира минималните категории PII, категории субекти на данни, източници и цели в REG02 и REG04 преди одобрение на дизайна за събиране или импорт.

4.2.2 [Both] The System Owner / Application Owner MUST конфигурира настройките за обработване по подразбиране до минималното събиране и обработване на PII, необходимо за документираната цел, и да запише доказателства в REG04 преди въвеждане в експлоатация.

4.2.3 [Controller] The Process Owner / Business Owner MUST документира незадължителните полета за PII, незадължителните избори за обработване и настройките, изключени по подразбиране, в REG02 и REG04 преди одобрение на потребителски интерфейс, формуляр или работен поток.

4.2.4 [Both] The System Owner / Application Owner MUST документира настройките по подразбиране за експониране на поверителността за изгледи, отчети, експорти, интерфейси и автоматизирани работни потоци в REG04 преди въвеждане в експлоатация.

4.2.5 [Both] The Process Owner / Business Owner MUST документира осъществимостта на деидентификация, псевдонимизация, агрегиране или обработване без идентифициране в REG04 преди одобряване на идентифицируема PII за тестване, анализи, докладване или вторична оперативна употреба.

4.2.6 [Both] The System Owner / Application Owner MUST документира обработването на временни артефакти с PII, включително временни файлове, кешове, журнали или междинни записи, в REG04 преди въвеждане в експлоатация.

4.2.7 [Both] The Process Owner / Business Owner MUST насочи изискванията за дизайн, за които отговарят PII10, PII11, PII13 или PII14, към съответния път за доказателства по свързаната политика в REG04 в срок до пет работни дни от идентифициране на зависимостта.

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Изключения

9.1 Изключения по дизайна за поверителност

9.1.1 [Both] The Process Owner / Business Owner MUST поиска изключение по дизайна за поверителност в REG12 преди одобряване на дизайн или промяна, които не могат да изпълнят приложимо изискване за дизайн за поверителност.

9.1.2 [Both] The Privacy Lead / PIMS Manager MUST оцени въздействието, компенсиращите контроли и срока на валидност на всяко изключение по дизайна за поверителност в REG12 в срок до пет работни дни от искането.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST запише становище в REG12 преди одобрение на изключение по дизайна за поверителност, включващо високорисково, чувствително, автоматизирано, мащабно, оспорвано или правно съществено обработване.

9.1.4 [All] Top Management MUST одобри изключение по дизайна за поверителност, което засяга обработване с висок ефект, обхват на сертификация, нерешен съществен риск или правно задължение, в REG12 преди изключението да влезе в сила.

9.1.5 [Both] The Privacy Lead / PIMS Manager MUST определи в REG12 срок на валидност, който не надвишава 90 дни, за всяко одобрено изключение по дизайна за поверителност преди одобрение.

9.1.6 [Both] The Privacy Lead / PIMS Manager MUST закрие или преоцени всяко изключение по дизайна за поверителност в REG12 в срок до пет работни дни от изтичане на срока му.

10. Прилагане на политиката

10.1 Прилагане на политиката и обработване на несъответствия

10.1.1 [Both] The Privacy Lead / PIMS Manager MUST запише липсващ преглед на дизайна за поверителност, липсващи доказателства за минимизиране, нерешен отказ на настройка по подразбиране или неоторизирано въвеждане в експлоатация като несъответствие в REG12 в срок до пет работни дни от идентифицирането.

10.1.2 [Both] The System Owner / Application Owner MUST предотврати въвеждането в експлоатация на система за обработване на PII, когато прегледът на дизайна за

поверителност в REG04 е непълен, и да запише решението в REG12 преди въвеждане в експлоатация.

10.1.3 [Both] The Vendor / Procurement Owner MUST предотврати въвеждането на доставчик или подписването на договор, когато изискваните доказателства за дизайн за поверителност в REG08 липсват, и да запише решението в REG12 преди въвеждане или подписване.

10.1.4 [Both] The Process Owner / Business Owner MUST спре използването на нов или променен дизайн за обработване на PII, докато прегледът в REG04, актуализациите в REG02 и изискваните изключения в REG12 не бъдат завършени.

10.1.5 [All] Top Management MUST изиска коригиращо действие в REG12 в срок до 10 работни дни при повтарящ се, продължителен или с висок ефект отказ в дизайна за поверителност.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST провери ефективността на коригиращото действие за несъответствия в дизайна за поверителност в REG12 при следващия планиран PIMS одит или в срок до 60 дни от закриването, което от двете настъпи първо.

11. Преглед и поддръжка

11.1 Преглед на политиката и контролите за дизайн

11.1.1 [All] The Privacy Lead / PIMS Manager MUST преглежда тази политика в REG12 ежегодно и в срок до 30 дни от съществена правна, свързана с обработването, технологична, свързана с обхвата на сертификация или с контрола на PIMS промяна.

11.1.2 [Both] The Process Owner / Business Owner MUST преглежда активните дейности по обработване в REG02 за промени в зависимостите на дизайна за поверителност ежегодно и в срок до 30 дни от съществена промяна в обработването.

11.1.3 [Both] The System Owner / Application Owner MUST преглежда доказателствата за конфигурация за поверителност по подразбиране в REG04 ежегодно и в срок до 30 дни от съществена системна промяна.

11.1.4 [Both] The Vendor / Procurement Owner MUST преглежда задълженията за дизайн за поверителност на доставчици, обработващи лични данни, подизпълнители по обработване и трети страни в REG08 преди подновяване и в срок до 30 дни от съществена промяна във взаимоотношенията.

11.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST прегледа въздействието върху поверителността на съществени промени в политиката в REG12 преди одобрение.

11.1.6 [All] Top Management MUST одобри съществените промени в тази политика в REG12 преди публикуване.

12. Свързани политики

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

12.2 PII02 - Политика за роли, отговорности и отчетност относно поверителността

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

12.4 PII04 - Политика за уведомление за поверителност и прозрачност

12.5 PII05 - Политика за управление на съгласията и предпочитанията

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

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

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

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

12.10 PII11 - Политика за точност и качество на PII

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

12.12 PII13 - Политика за международен трансфер на PII

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

12.14 PII17 - Политика за документирана информация и управление на доказателствата в PIMS

12.15 PII18 - Политика за мониторинг, одит и подобрение в 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 подпомагат.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.2; Clause 6.1.3** - Съпоставено с проверка на риска за поверителността, връзка с действия за третиране, анализ на зависимостите в дизайна, ескалация и коригиращо действие, без да се дублира пълната методология за риск за поверителността и DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].

13.2.2 **Clause 6.3; Clause 8.1** - Съпоставено с планирани промени в поверителността, започване на проект, оперативен преглед на дизайна за поверителност, контрол при въвеждане в експлоатация и преглед при съществени промени. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].

13.2.3 **Clause 7.5** - Съпоставено с документирани доказателства за дизайн за поверителност, съхранявани в REG02, REG04, REG08 и REG12. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1; Clause 10.2** - Съпоставено с показатели за дизайн за поверителност, извадкова проверка на доказателства, записване на несъответствия, коригиращо действие и проверка на ефективността. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].

13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Съпоставено с документиране на целите на обработването, записите за обработване, връзката с дизайна за поверителност и критериите за задействане на риск за поверителността или проверка за необходимост от DPIA за обработване от администратор. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Съпоставено с ограничаване на събирането и обработването на PII чрез основани на целта минимални изисквания за данни, незадължително обработване, изключено по подразбиране, и минимални настройки за обработване по подразбиране. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].

13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Съпоставено с насочване на зависимостите от точността, цели за минимизиране, осъществимост на деидентификацията и доказателства за дизайн за минимизиране на идентифицируемата PII. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].

13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Съпоставено с идентифициране на етап дизайн на деидентификация, зависимост от изтриване, временни артефакти с PII и насочване към

контроли на жизнения цикъл, без да се дублира изпълнението на съхранение или унищожаване. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].

13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Съпоставено с нареждания на клиента към обработващия лични данни, информация за поддръжка на клиента, записи за дизайн на обработващия лични данни и одобрени от клиента промени в дизайна на услугата. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].

13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Съпоставено с възможности за дизайн на обработващия лични данни за временни файлове, зависимост от връщане или унищожаване и зависимост от контрол на предаването, записани като доказателства за дизайн, без да се дублират оперативните процедури за изтриване или контролите за сигурност. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].

13.2.11 **Annex A.3.27; Annex A.3.29** - Съпоставено с изисквания за поверителност в жизнения цикъл на разработката, инженерни принципи, контролни точки за защита на PII и доказателства за конфигурация за поверителност по подразбиране. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Съпоставено с ограничаване на целите, минимален дизайн за PII, връзка със записите за обработване, минимизиране по подразбиране, доказателства и отчетност. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Съпоставено с мерки на администратора, управленски преглед, одобрение на изключения, коригиращо действие и поддръжка на политиката за внедряване на защита на личните данни още при проектиране. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].

13.3.3 **Article 25** - Съпоставено със започване на проект, изисквания за поверителност на етап дизайн, настройки за поверителност по подразбиране, минимизиране, проверки на дизайна при набавяне, преглед при въвеждане в експлоатация и преглед, задействан от промяна. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].

13.3.4 **Article 28** - Съпоставено с нареждания към обработващия лични данни, поддръжка за дизайн от обработващия лични данни, доказателства за дизайн за поверителност на доставчика и одобрени от клиента промени в дизайна. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].

13.3.5 **Article 30** - Съпоставено с връзка със записите за обработване, актуализации в REG02, зависимости на дизайна на дейностите по обработване и доказателства за записи за обработване. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.3.6 **Article 35** - Съпоставено с критерии за задействане на риск за поверителността и проверка за необходимост от DPIA на етап дизайн, становище при висок риск и проверки след внедряване, без да се дублира методологията за DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7** - Съпоставено с идентифициране на контроли за поверителност на етап проектиране, връзка с риска за поверителността и доказателства за дизайн за внедряване на контролите. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].

13.4.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Съпоставено с определяне на целта, ограничаване на събирането, минимизиране на данните, ограничено използване и

настройки за обработване по подразбиране. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].

13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Съпоставено с насочване на зависимостите от точността, доказателства за отчетност, мониторинг на дизайна за поверителност, одит и коригиращо действие. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Съпоставено с легитимност на целта, ограничаване на събирането, минимизиране на данните, ограничаване на използването и разкриването, зависимост от съхранение, обработване на временни файлове и контроли за дизайн, свързани със зависимостите от точността. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].