					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII21					Заглавие на документа: **Политика за поверителност при изкуствен интелект и автоматизирано вземане на решения**							
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**

Правна бележка (авторски права и ограничения за ползване)

(C) 2025 Clarysec LLC. All rights reserved.

Настоящият документ е интелектуална собственост на Clarysec LLC. Никоя част от него не може да бъде копирана, използвана повторно, разпространявана или изменяна за търговски или внедрителски цели без изрично писмено разрешение.

Неупълномощеното използване е строго забранено и може да доведе до правни действия.

За лицензиране се свържете с: info@clarysec.com

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 относно обработване чрез AI, профилиране и автоматизирано вземане на решения
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Мониторинг, несъответствие и коригиращо действие за контроли за поверителност при AI
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Цел, правно основание, оценка на въздействието върху поверителността и записи на администратора
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Договори с обработващи лични данни и отговорности на съвместен администратор при свързано с AI обработване на PII
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Задължения към субектите на данни и прозрачност при свързано с AI обработване
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Възражение, достъп, коригиране, изтриване, обработване на искания и задължения при автоматизирано

				вземане на решения
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 при входни данни, изходни резултати и производни данни за AI
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Международно прехвърляне, разкриване и маршрутизиране на искания за разкриване за свързана с AI PII
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Споразумение с обработващ лични данни, документирани нареждания, подкрепа за задълженията на клиента и записи
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Подкрепа от обработващия лични данни за задълженията към субектите, маршрутизиране на трансфери и обработване на разкриване
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Защита на записи и журнализиране, свързани със свързано с AI обработване на PII
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Профилиране, справедливост, прозрачност, ограничаване на целите, минимизиране, точност и отчетност
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Законосъобразност, данни от специални

				категории и предпазни мерки за данни за присъди или нарушения
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Прозрачна информация, достъп и съдържателна информация относно автоматизирано вземане на решения
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Поправяне, изтриване, ограничаване, възражение и права при автоматизирано вземане на решения
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Отговорност на администратора, защита още при проектиране/по подразбиране, съвместни администратори, обработващи лични данни, записи, сигурност, DPIA и задачи на DPO
GDPR	Article 44	Conditional	Referenced	Маршрутизиране на международни трансфери при свързано с AI обработване на PII
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Принципи за цел, събиране, минимизиране, използване, съхранение, разкриване, точност и качество
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Прозрачност, участие на физическото лице, отчетност, информационна сигурност и

				съответствие в областта на поверителността
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Полза от PIA, определяне на праг и подготовка за оценка на риска за поверителността, свързана с AI
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Контроли за цел, събиране, минимизиране, използване, съхранение, разкриване, точност и участие на субекта

1. Обхват

1.1 Тази политика определя задължителните изисквания за поверителност при дейности по обработване чрез изкуствен интелект, профилиране, точкова оценка, препоръчване, подпомагане при вземането на решения и автоматизирано вземане на решения, които използват, извеждат, генерират, разкриват или по друг начин обработват PII в обхвата на PIMS.

1.2 Тази политика се прилага за:

1.2.1 AI-enabled системи, приложения, модели, услуги, работни потоци, двигатели за вземане на решения, инструменти за точкова оценка, препоръчващи системи, аналитични модели и процеси за автоматизирано вземане на решения, които обработват PII;

1.2.2 профилиране, сегментиране, класификация, прогнозиране, извеждане на заключения, персонализация, ранжиране, допустимост, откриване на измами, точкова оценка на риска, решения за достъп, оценки, свързани със заетостта, профилиране, свързано с деца, маркетингова персонализация и сходно обработване, когато е включена PII;

1.2.3 свързана с AI PII, използвана за обучение, тестване, валидация, настройване, мониторинг, продукционно извеждане, преглед на изходни резултати, измерване на резултатността, разследване на инциденти или извеждане на модел от употреба;

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

1.2.5 свързани с AI доставчици, обработващи лични данни, подизпълнители по обработване, получатели при споделяне на данни и маршрути за международен трансфер, които обработват PII.

1.3 Тази политика не създава цялостна рамка за управление на AI, система за управление на AI, инвентар на AI, инвентар на модели, регистър на риска на модели, регистър на справедливостта, регистър на алгоритми, регистър на инциденти с AI, комитет за AI, роля на собственик на модел, роля на собственик на AI система, работен поток за правни становища или отделен формуляр за одобрение на AI.

1.4 Тази политика не заменя:

1.4.1 PII03 за инвентар на обработването, правно основание и собственост върху ROPA;

1.4.2 PII04 за управление на уведомленията за поверителност;

1.4.3 PII05 за управление на съгласията и предпочитанията;

1.4.4 PII06 за работния поток за правата на субектите на данни;

1.4.5 PII07 за оценката на риска за поверителността и методологията за DPIA;

1.4.6 PII08 за контролните точки за защита на личните данни още при проектиране и по подразбиране;

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

1.4.8 PII10 за изпълнението на съхранение, изтриване и унищожаване;

1.4.9 PII11 за контролите за точност и качество;

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

1.4.11 PII13 за контролите за международни трансфери;

1.4.12 PII14 за сигурността и контрола на достъпа;

1.4.13 PII15 за обработването на инциденти и нарушения;

1.4.14 PII18 за мониторинга, одита и подобрението;

1.4.15 PII19 за поверителността на служителите;

1.4.16 PII20 за поверителността на децата;

1.4.17 PII22 за маркетинговата поверителност и бисквитките.

2. Цел

2.1 Целта на тази политика е да гарантира, че дейностите с AI, профилиране и автоматизирано вземане на решения, включващи PII, се идентифицират, документират, оценяват от гледна точка на риска, правят прозрачни и оспорими, наблюдават и контролират чрез PIMS, без да се създават дублиращи артефакти за управление, специфични за AI.

2.2 Тази политика гарантира, че задълженията за поверителност при свързано с AI обработване на PII се доказват чрез REG02, REG04, REG06, REG07, REG08, REG09, REG10 и REG12.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 идентифицира обработването чрез AI, профилиране и автоматизирано вземане на решения, включващо PII, в REG02;

3.1.2 документира свързаните с AI цели, правно основание, категории PII, източници на данни, изведени данни, изходни резултати, получатели и ефекти от решенията в REG02;

3.1.3 задейства проверка на риска за поверителността и маршрутизиране на DPIA чрез REG04;

3.1.4 гарантира, че свързаните с AI уведомления за поверителност и съдържателна информация се записват в REG07;

3.1.5 маршрутизира исканията за права, възражения, човешки преглед и оспоримост чрез REG06;

3.1.6 контролира свързаните с AI обработващи лични данни, подизпълнители по обработване, доставчици и договорености за споделяне на данни чрез REG08;

3.1.7 маршрутизира свързаните с AI международни трансфери чрез REG09;

3.1.8 ескалира подозирани свързани с AI инциденти с PII, неправомерна употреба, неоторизирано разкриване и неблагоприятни резултати за поверителността чрез REG10 и REG12;

3.1.9 записва мониторинг, изключения, несъответствия, коригиращи действия и подобрения в REG12.

4. Декларации на политиката

4.1 Идентифициране на AI, профилиране и автоматизирано вземане на решения

4.1.1 [Controller] Когато се предлага нова или съществено променена система, приложение, модел, работен поток, услуга или бизнес процес, Process Owner / Business Owner трябва да определи дали тя използва AI, профилиране, точкова оценка, препоръчване, подпомагане при вземането на решения или автоматизирано вземане на решения, включващо PII, и да запише определянето в REG02.

4.1.2 [Controller] Преди да започне свързано с AI обработване на PII, Process Owner / Business Owner трябва да документира целта на обработването, категориите PII, категориите субекти на данни, източниците на данни, категориите изведени или производни данни, категориите изходни резултати, категориите получатели, правното основание и връзката със сроковете за съхранение в REG02.

4.1.3 [Controller] Преди профилиране, точкова оценка, препоръчване, подпомагане при вземането на решения или автоматизирано вземане на решения да се използва в

продукционна среда, Process Owner / Business Owner трябва да документира контекста на решението, очаквания ефект върху субектите на данни, човешкото участие и маршрута за права в REG02 и REG04.

4.1.4 [Joint Controller] Преди свързано с AI обработване на PII да се извършва със съвместен администратор, Privacy Lead / PIMS Manager трябва да документира отговорността за определяне на целта, уведомление, обработване на права, подкрепа за DPIA, управление на обработващи лични данни и ескалация на инциденти в REG08.

4.1.5 [Processor] Преди обработване на PII чрез свързана с AI услуга за клиент, Process Owner / Business Owner трябва да потвърди, че нарежданията на клиента, разрешените цели, забранените употреби, обработването на изходни резултати и задълженията за съдействие са документирани в REG08.

4.1.6 [Both] Преди да се активира свързано с AI обработване на PII, Privacy Lead / PIMS Manager трябва да потвърди, че обработването е свързано с приложимите канонични доказателствени обекти и че не се създава отделен специфичен за AI регистър извън REG02, REG04, REG06, REG07, REG08, REG09, REG10 или REG12.

4.2 Оценка на риска за поверителността и маршрутизиране на DPIA

4.2.1 [Controller] Преди стартиране или съществена промяна на свързано с AI обработване на PII, Privacy Lead / PIMS Manager трябва да извърши проверка на риска за поверителността и да запише решението за DPIA в REG04.

4.2.2 [Conditional] Когато свързаното с AI обработване включва профилиране, автоматизирани решения, мащабно оценяване, данни от специални категории, данни за присъди и нарушения, уязвими субекти на данни, оценяване на служители, деца, поведенчески мониторинг, данни за местоположение, биометрични данни, точкова оценка с високо въздействие или значителни ефекти, Data Protection Officer / Privacy Advisor трябва да прегледа риска за поверителността и да запише становището в REG04.

4.2.3 [Controller] Преди въвеждане в продукционна експлоатация на свързано с AI обработване на PII, Process Owner / Business Owner трябва да документира действията за третиране на риска, статуса на остатъчния риск и доказателства за готовност за въвеждане в експлоатация в REG04 или REG12.

4.2.4 [Controller] Преди PII да бъде използвана повторно за обучение, тестване, валидация, настройване, мониторинг или подобрение на модел за нова или съществено променена цел, Process Owner / Business Owner трябва да извърши преглед за поверителност и да запише решението в REG02 и REG04.

4.2.5 [Conditional] Когато остатъчният риск за поверителността остава висок след планираното третиране, Top Management трябва да одобри, отхвърли или изиска допълнително третиране преди продукционна употреба и да запише решението в REG04 и REG12.

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

9. Изключения

9.1 [All] Преди отклонение от свързано с AI изискване за поверителност в тази политика, заявяващият Process Owner / Business Owner трябва да подаде обосновка за изключение и доказателства за компенсиращ контрол в REG12.

9.2 [Conditional] Когато изключение засяга профилиране, автоматизирано вземане на решения, човешки преглед, оспоримост, прозрачност, резултат от DPIA, точкова оценка с високо въздействие, обработване, свързано с деца, обработване, свързано със служители, ограничения за обработващи лични данни или международни трансфери, Data Protection

Officer / Privacy Advisor трябва да прегледа изключението и да запише становището в REG04 или REG12.

9.3 [Conditional] Когато изключение създава или запазва висок остатъчен риск за поверителността, Top Management трябва да одобри или отхвърли изключението и да запише решението в REG04 и REG12.

9.4 [All] Преди одобрено свързано с AI изключение за поверителност да изтече, Privacy Lead / PIMS Manager трябва да прегледа статуса на закриване, подновяване или коригиращо действие и да запише резултата в REG12.

10. Прилагане на политиката

10.1 [All] Когато бъде установено неспазване на тази политика, Privacy Lead / PIMS Manager трябва да запише несъответствието и коригиращото действие в REG12.

10.2 [Both] Когато се подозира неоторизирано свързано с AI обработване на PII, разкриване, достъп, неправомерно използване на модел, неуспех при права или неблагоприятен резултат за поверителността, Incident Response Coordinator трябва да инициира ескалация на инцидента и да запише доказателства в REG10 и REG12.

10.3 [Both] Когато обработващ лични данни, подизпълнител по обработване, доставчик или получател при споделяне на данни не изпълни свързани с AI задължения за поверителност, Vendor / Procurement Owner трябва да запише действие за отстраняване, ескалация или прекратяване в REG08 и REG12.

10.4 [All] Когато възникнат повтарящи се или системни свързани с AI несъответствия в поверителността, Top Management трябва да прегледа въпроса и да запише управленското действие в REG12.

11. Преглед и поддръжка

11.1 [All] Най-малко веднъж годишно Privacy Lead / PIMS Manager трябва да преглежда тази политика за продължаваща пригодност и да записва резултата от прегледа в REG12.

11.2 [Conditional] Когато закони, услуги, модели, източници на данни, практики за профилиране, логика за автоматизирано вземане на решения, договорености с доставчици, маршрути за трансфер или рискове за поверителността се променят съществено, Privacy Lead / PIMS Manager трябва да прегледа засегнатите свързани с AI контроли за поверителност и да запише резултата в REG02, REG04 или REG12.

11.3 [Controller] Най-малко веднъж годишно и след съществени промени в свързано с AI потребителско пътуване, Process Owner / Business Owner трябва да прегледа доказателствата за прозрачност, съдържателна информация, човешки преглед и маршрут за права и да запише прегледа в REG06 и REG07.

11.4 [All] След закриване на свързани с AI коригиращи действия за поверителност Internal Audit / Compliance Reviewer трябва да провери ефективността и да запише доказателства за проверката в REG12.

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 в областта на поверителността

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

12.4 PII04 - Политика за уведомления за поверителност и прозрачност

12.5 PII05 - Политика за управление на съгласията и предпочитанията

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 защита на личните данни 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 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 до PII

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

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

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

12.18 PII19 - Политика за поверителност на служителите

12.19 PII20 - Политика за поверителност на децата

12.20 PII22 - Политика за маркетингова поверителност и бисквитки

13. Референтни стандарти и рамки

13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].

13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].

13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].

13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].

13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].

13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].

13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].

13.8 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.3; 4.7.4; 4.7.5; 7.7].

13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].

13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].

13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].

13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].

13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].

13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].

13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].

13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].

13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].

13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].

13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].

13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].

13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].