					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII07					Заглавие на документа: **Политика за оценка на риска за поверителността и DPIA**							
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 6.1.1	Both	Primary	Рискове и възможности в PIMS
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Оценка на риска за поверителността
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Третиране на риска за поверителността и връзка със SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Планирани промени в PIMS и повторна оценка на риска
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Документирана информация за риска за поверителността и DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Оперативно планиране и контрол
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Оперативна оценка на риска за поверителността
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Оперативно третиране на риска за поверителността
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Мониторинг и измерване на риска за поверителността
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Преглед от ръководството на риска за поверителността
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Несъответствие и коригиращо действие, свързани с риска

ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Оценка на въздействието върху поверителността
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Записи за обработването, подпомагащи оценката на риска
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Споразумение с клиент на обработващ лични данни и съдействие за DPIA
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Информация от обработващ лични данни в подкрепа на съответствието на клиента
GDPR	Article 5(2)	Controller	Supporting	Доказателства за отчетност
GDPR	Article 24	Controller	Supporting	Отговорност и мерки на администратора
GDPR	Article 25	Controller	Supporting	Защита на данните още при проектиране и по подразбиране
GDPR	Article 28	Both	Supporting	Съдействие от обработващия лични данни и нареждания
GDPR	Article 30	Both	Supporting	Записи за обработването в подкрепа на DPIA
GDPR	Article 32	Both	Supporting	Риск за сигурността и предпазни мерки
GDPR	Article 35	Controller	Primary	Оценка на въздействието върху защитата на данните
GDPR	Article 36	Controller	Primary	Предварителна консултация

GDPR	Article 39	Conditional	Supporting	Становище и мониторинг от DPO, когато е приложимо
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Контроли за поверителност, информационна сигурност и съответствие с изискванията за поверителност
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Обхват, ползи, критерий за задействане и подготовка за PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Програма за защита на PII и идентифициране на изисквания
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Интегриране на управлението на организационния риск за поверителността

1. Обхват

1.1 Тази политика определя изискванията за оценка на риска за поверителността, проверка за необходимост от DPIA, изпълнение на пълна DPIA, третиране на риска, приемане на остатъчния риск, консултация, преглед и управление на доказателства за обработването на PII в обхвата на PIMS.

1.2 Тази политика се прилага за:

1.2.1 нови и съществено променени дейности по обработване на PII;

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

1.2.3 системи, приложения, услуги, бизнес процеси, доставчици, обработващи лични данни, подизпълнители по обработване, международни трансфери и механизми за споделяне на данни, които засягат обработването на PII;

1.2.4 доказателства за риска за поверителността и DPIA, поддържани в REG04, и поддържащи доказателства, поддържани в REG02, REG03, REG08, REG09, REG10, REG11 и REG12.

1.3 Тази политика не заменя контролите за инвентара на обработването, контролите за уведомленията за поверителност, контролите за съгласие, контролите за правата на субектите на данни, контролите за поверителност още при проектиране, контролите за доставчици, контролите за международни трансфери, контролите за сигурност на PII, контролите за инциденти, контролите за документирана информация или контролите за мониторинг/одит/подобрение. Тези изисквания са определени в свързаните политики, посочени в раздел 12.

1.4 За целите на тази политика оценка на риска за поверителността означава документирано идентифициране, анализ, оценяване, третиране, преглед и мониторинг на потенциални неблагоприятни въздействия върху поверителността, произтичащи от обработването на PII.

1.5 За целите на тази политика DPIA означава документирана оценка, използвана при обработване от администратор, което е вероятно да доведе до висок риск за субектите на данни и която оценява необходимостта, пропорционалността, рисковете, предпазните мерки, остатъчния риск, нуждите от консултация и условията за одобрение.

1.6 За целите на тази политика висок остатъчен риск за поверителността означава риск за поверителността, който остава над одобрения праг за приемане след предложено или внедрено третиране на риска.

1.7 За целите на тази политика съществена промяна означава всяка промяна, засягаща обхвата на PIMS, целта на обработването, правното основание, категориите PII, категориите субекти на данни, мащаба на обработването, технологията за обработване, мониторинга или профилирането, автоматизираното вземане на решения, уязвимите субекти на данни, получателите, обработващите лични данни, подизпълнителите по обработване, международните трансфери, срока за съхранение, контролите за сигурност, рисковия профил, нарежданията на клиента или сертификационния обхват.

2. Цел

2.1 Целта на тази политика е да гарантира, че рисковете за поверителността и задълженията за DPIA се идентифицират, оценяват, третират, одобряват, преглеждат и доказват, преди обработването на PII да създаде неприемлив риск за субектите на данни или за PIMS.

2.2 Тази политика позволява на организацията да демонстрира управление на поверителността, основано на риска, отчетност на администратора за DPIA, съдействие от обработващия лични данни за DPIA, документирано третиране на риска, одобрение на остатъчния риск,

вземане на решения за предварителна консултация и непрекъснато подобрение на контролите за поверителност.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 определя задължителни критерии за задействане на скрининг на риска за поверителността;

3.1.2 определя кога се изисква пълна DPIA;

3.1.3 гарантира, че решенията на администратора относно DPIA са документирани и подлежат на преглед;

3.1.4 гарантира, че съдействието за DPIA от обработващи лични данни и подизпълнители по обработване е документирано, когато се изисква от нареждане на клиента или от споразумение;

3.1.5 гарантира, че рисковете за поверителността се оценяват, преди да започне ново или съществено променено обработване на PII;

3.1.6 гарантира, че мерките за третиране на риска за поверителността се възлагат, изпълняват и проверяват;

3.1.7 гарантира, че високите остатъчни рискове за поверителността се ескалират и одобряват, преди обработването да започне или да продължи;

3.1.8 гарантира, че решенията за предварителна консултация се документират, когато остава висок остатъчен риск;

3.1.9 гарантира, че доказателствата за риска за поверителността и DPIA се поддържат в REG04 и са свързани със съответните доказателствени обекти;

3.1.10 избягва създаването на отделни регистри за DPIA, риск или консултации извън REG04.

4. Положения на политиката

4.1 Скрининг на риска за поверителността

4.1.1 [Both] Process Owner / Business Owner трябва да инициира скрининг на риска за поверителността в REG04, преди да започне ново или съществено променено обработване на PII, записано в REG02.

4.1.2 [Both] Privacy Lead / PIMS Manager трябва да поддържа критерии за скрининг на риска за поверителността в REG04 преди първоначалната експлоатация на PIMS и ежегодно след това.

4.1.3 [Controller] Process Owner / Business Owner трябва да завърши проверка за необходимост от DPIA в REG04, преди да започне обработване от администратор, което отговаря на критериите за скрининг на риска за поверителността.

4.1.4 [Processor] Vendor / Procurement Owner трябва да запише изискванията на клиента за съдействие при DPIA в REG08, преди да започне обработване от обработващ лични данни, когато споразумението с клиента или документираното нареждане изисква съдействие за DPIA.

4.1.5 [Both] System Owner / Application Owner трябва да предостави доказателства за системен дизайн, достъп, сигурност, журнализиране и поток на данни в REG04 преди одобрението на оценката на риска за поверителността за нови или съществено променени системи, обработващи PII.

4.1.6 [Both] Privacy Lead / PIMS Manager трябва да запише резултата от скрининга и обосновката на решението за пълна DPIA в REG04, преди дейността по обработване да продължи.

4.2 Критерии за задействане на DPIA и определяне на изискването

4.2.1 [Controller] Privacy Lead / PIMS Manager трябва да изисква пълна DPIA в REG04, преди да започне обработване от администратор, което е вероятно да доведе до висок риск.

4.2.2 [Controller] Process Owner / Business Owner трябва да насочи към Privacy Lead / PIMS Manager в REG04 обработване, включващо голям мащаб, систематичен мониторинг, профилиране, автоматизирани решения, специални категории PII, данни за присъди или нарушения, уязвими субекти на данни, иновативна технология или съществено променено обработване, преди обработването да започне.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor трябва да запише становище в REG04 преди одобрението на решение за изискване на пълна DPIA за високорисково обработване от администратор.

4.2.4 [Both] Process Owner / Business Owner трябва повторно да извърши скрининг на риска за поверителността в REG04, преди да използва PII за нова цел, да добави нов получател, да въведе нов обработващ лични данни или подизпълнител по обработване, да промени системната архитектура или да започне нов международен трансфер.

4.2.5 [Processor] Privacy Lead / PIMS Manager трябва да документира дали се изисква съдействие от обработващия лични данни за DPIA в REG08 в срок до 10 работни дни от получаване на искане от клиент за съдействие при DPIA.

4.2.6 [Subprocessor] Vendor / Procurement Owner трябва да документира изискванията за съдействие при DPIA нагоре по веригата в REG08, преди да започне подизпълнение по обработване, когато клиентът нагоре по веригата или споразумението с обработващия лични данни изисква такова съдействие.

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

9. Изключения

9.1 Изключения за риска за поверителността и DPIA

9.1.1 [All] Process Owner / Business Owner трябва да поиска всяко изключение от тази политика в REG12, преди отклонението да настъпи.

9.1.2 [All] Privacy Lead / PIMS Manager трябва да оцени въздействието върху поверителността, правните аспекти, сертификацията, операциите и субектите на данни за всяко поискано изключение в REG04 или REG12 в срок до 10 работни дни от искането.

9.1.3 [All] Data Protection Officer / Privacy Advisor трябва да запише становище в REG12 преди одобрението на всяко изключение, което засяга високорисково обработване, завършване на пълна DPIA, предварителна консултация, висок остатъчен риск за поверителността или съдействие на клиент за DPIA.

9.1.4 [All] Top Management трябва да одобри в REG12 изключения по риска за поверителността или DPIA, които засягат високорисково обработване, сертификационен обхват, предварителна консултация или неразрешен висок остатъчен риск за поверителността, преди изключението да влезе в сила.

9.1.5 [All] Privacy Lead / PIMS Manager трябва да зададе дата на изтичане, която не надвишава 90 дни, в REG12 за всяко одобрено изключение по риска за поверителността или DPIA преди одобрение.

9.1.6 [All] Process Owner / Business Owner трябва да закрие или повторно да оцени всяко изключение по риска за поверителността или DPIA в REG12 в срок до пет работни дни от изтичането му.

10. Прилагане на политиката

10.1 Прилагане на изискванията за риска за поверителността и DPIA

10.1.1 [All] Privacy Lead / PIMS Manager трябва да запише липсващи, неточни, непълни, просрочени или неодобрени доказателства за риска за поверителността или DPIA в REG04 като несъответствие в REG12 в срок до пет работни дни от идентифицирането.

10.1.2 [Controller] Process Owner / Business Owner трябва да спре ново високорисково обработване от администратор, когато изискваните доказателства за одобрение на DPIA в REG04 липсват преди стартиране.

10.1.3 [Both] System Owner / Application Owner трябва да блокира въвеждането в експлоатация на системи, обработващи PII, когато изискваните доказателства за третиране на риска в REG04 липсват преди одобрение за въвеждане в експлоатация.

10.1.4 [Both] Vendor / Procurement Owner трябва да блокира въвеждането на доставчик, обработващ лични данни, подизпълнител по обработване или механизъм за споделяне на данни, когато изискваните доказателства за риска за поверителността или съдействие за DPIA в REG04 липсват преди одобрение на споразумението.

10.1.5 [All] Top Management трябва да преглежда неразрешените съществени несъответствия, свързани с риска за поверителността или DPIA, в REG12 по време на прегледа от ръководството.

10.1.6 [All] Privacy Lead / PIMS Manager трябва да ескалира повтарящи се пропуснати срокове за скрининг в REG04, преглед на DPIA или третиране на риска към Top Management в REG12 в срок до пет работни дни след второто възникване в рамките на 12-месечен период.

10.1.7 [All] Internal Audit / Compliance Reviewer трябва да провери ефективността на коригиращите действия за несъответствия, свързани с риска за поверителността и DPIA, в REG12 при следващия планиран одит или в срок до 60 дни от закриването, което от двете настъпи по-рано.

11. Преглед и поддръжка

11.1 Преглед и поддръжка на политиката

11.1.1 [All] Privacy Lead / PIMS Manager трябва да преглежда тази политика в REG12 ежегодно и в срок до 30 дни от съществена промяна в изискванията за риска за поверителността, DPIA, предварителна консултация, съдействие от обработващ лични данни или сертификация.

11.1.2 [All] Privacy Lead / PIMS Manager трябва ежегодно да преглежда критериите за скрининг в REG04, критериите за задействане на DPIA, критериите за рейтинг на риска и критериите за приемане на остатъчния риск в REG12.

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

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

11.1.5 [All] Privacy Lead / PIMS Manager трябва да актуализира REG03 и REG04 в срок до 15 работни дни след одобрени промени в политиката, които променят приложимостта на контролите, критериите за риск или изискванията за проверка за необходимост от DPIA.

11.1.6 [All] Privacy Lead / PIMS Manager трябва да запише комуникацията на одобрените промени в тази политика 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 във връзка с поверителността

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

12.5 PII04 - Политика за уведомления за поверителност и прозрачност

12.6 PII05 - Политика за управление на съгласия и предпочитания

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

12.8 PII08 - Политика за поверителност 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 на PII и контрол на достъпа

12.15 PII15 - Политика за управление на инциденти и нарушения, свързани 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

13. Референтни стандарти и рамки

13.1 Тази политика е съпоставена със следните стандарти и регулации. Съпоставянето обяснява как политиката подпомага посочените изисквания и идентифицира вътрешните клаузи, които ги изпълняват или подпомагат.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Съпоставено с идентифициране и планиране на действия за рискове и възможности, свързани с поверителността, чрез критерии за скрининг, прагове за риск, ескалация и входни данни за преглед от ръководството. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Съпоставено с извършване на скрининг на риска за поверителността, оценка на риска за поверителността, рейтинг на риска, повторна оценка и оценяване на критерии за задействане на DPIA, преди ново или съществено променено обработване да продължи. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Съпоставено с планиране на третиране на риска за поверителността, актуализации на приложимостта на контролите, изпълнение на третиране, приемане на остатъчния риск и връзка със SoA. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Съпоставено с планирани промени в PIMS и обработването, които задействат повторна оценка на риска за поверителността и преглед на DPIA. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Съпоставено с контролирана документирана информация за скрининг на риска за поверителността, доказателства за DPIA, третиране на риска, приемане на остатъчния риск, решения за предварителна консултация, изключения, несъответствия и доказателства за преглед на политиката. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Съпоставено с оперативно изпълнение на контролите за риска за поверителността и DPIA преди въвеждане в експлоатация, въвеждане на доставчици, одобрение на обработване, приключване на третиране и връзка с коригиращи действия. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Съпоставено с оперативна оценка на риска за поверителността за нови, променени, системни, доставчически, трансферни и породени от инциденти промени в обработването. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Съпоставено с оперативно третиране на риска за поверителността, възлагане на третиране, изпълнение на третиране, ескалация на просрочено третиране и проверка на ефективността. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Съпоставено с мониторинг и измерване на покритието на скрининга, статуса на DPIA, откритите рискове, просрочените действия за третиране, действията на доставчици, действията за третиране на риска за сигурността, действията за повторна оценка след инциденти и одитните констатации. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Съпоставено с преглед от ръководството на високи остатъчни рискове за поверителността, просрочени действия за третиране, статус на пълни DPIA, решения за предварителна консултация и съществени изключения по риска за поверителността. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Съпоставено с несъответствия, свързани с риска за поверителността и DPIA, изключения, откриване на коригиращи действия, ескалация и проверка на ефективността. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Съпоставено с оценяване на необходимостта от и прилагане, когато е подходящо, на оценка на въздействието върху поверителността за ново или променено обработване от администратор. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Съпоставено със записи за обработването, подпомагащи входните данни за оценка на риска за поверителността и DPIA, включително цел, категории, системи, получатели, трансфери и доставчици. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Съпоставено със споразумения с клиенти на обработващ лични данни и задължения за съдействие на клиента при DPIA. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Съпоставено с предоставяне от обработващия лични данни на информация, необходима за съответствието на клиента, включително съдействие при DPIA и доказателства за клиентска поддръжка. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Съпоставено с доказателства за отчетност за проверка за необходимост от DPIA, решения за пълна DPIA, третиране на риска, приемане на остатъчния риск, решения за предварителна консултация, изключения, одитни констатации и коригиращи действия. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Съпоставено с отговорността на администратора за подходящи мерки спрямо риска за поверителността, преглед на висок остатъчен риск, одобрение от ръководството и поддръжка на политиката. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Съпоставено с доказателства за защита на личните данни още при проектиране и по подразбиране, използвани при оценка на риска и преди одобрение за въвеждане в експлоатация. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Съпоставено със съдействие от обработващи лични данни и подизпълнители по обработване при DPIA, обработване на нареждания на клиенти и доказателства за третиране на риска, свързан с доставчици. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Съпоставено със записи за обработването, подпомагащи входните данни за оценката на риска за поверителността и DPIA. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Съпоставено с входни данни за риска за сигурността на PII, избор на предпазни мерки, третиране на риска за сигурността и актуализации на статуса на контролите за сигурност. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Съпоставено с проверка за необходимост от DPIA, определяне на изискване за пълна DPIA, съдържание на DPIA, становище на DPO, преглед и блокиране на високорисково обработване без изисквано одобрение на DPIA. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Съпоставено с вземане на решения за предварителна консултация, становище на DPO, одобрение от Top Management и действия за продължаване, спиране, препроектиране или консултация, когато остава висок остатъчен риск. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Съпоставено със становище и мониторинг от Data Protection Officer / Privacy Advisor, когато е приложимо, за решения относно DPIA, високорисково обработване, предварителна консултация и промени в политиката. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Съпоставено с идентифициране на контроли за поверителност, предпазни мерки за сигурност, съответствие с изискванията за поверителност, доказателства за риска за поверителността, мониторинг и преглед. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Съпоставено с обхвата на процеса PIA, ползите, определянето на критерии за задействане, подготовката, входните данни за оценката, доказателствата от заинтересовани страни и структурата на доклада за DPIA, поддържани в REG04. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Съпоставено с изискванията към програмата за защита на PII, идентифицирането на изисквания за защита на PII, избора на контроли, основан на риска, и връзката с третирането на риска за поверителността. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Съпоставено с принципите за организационен риск за поверителността, лидерство, интеграция, оценка на риска, третиране на риска, мониторинг и преглед, както и записване и докладване. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].