					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII15					Заглавие на документа: **Политика за управление на инциденти и нарушения на сигурността на личните данни**							
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 7.4; Clause 7.5	Both	Supporting	Комуникации в PIMS и документирани доказателства за нарушения
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Оперативен контрол, оценка на риска за поверителността и връзка с третирането
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Мониторинг, оценяване, несъответствие, коригиращо действие и подобрение
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Планиране и подготовка за управление на инциденти при обработване на PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Реагиране при инциденти по информационна сигурност, включващи PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Правни, законоустановени, регулаторни и договорни изисквания и защита на записите
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Споразумение с клиента на обработващия лични данни и подкрепа за задълженията на клиента
GDPR	Article 5(2); Article 24	Controller	Supporting	Отчетност и отговорност на администратора

GDPR	Article 26	Joint Controller	Supporting	Координация на отговорностите при нарушение между съвместни администратори
GDPR	Article 28	Both	Supporting	Съдействие от обработващия лични данни и договорни задължения на обработващия лични данни
GDPR	Article 32	Both	Supporting	Сигурност на обработването и способност за откриване на нарушения
GDPR	Article 33	Both	Primary	Уведомяване за нарушение на сигурността на личните данни и документиране на нарушението
GDPR	Article 34	Controller	Primary	Съобщаване на нарушения на сигурността на личните данни на засегнатите субекти на данни
GDPR	Article 39	Conditional	Supporting	Консултации от DPO, мониторинг, сътрудничество и подкрепа като точка за контакт
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Принципи на информационна сигурност и съответствие в областта на поверителността
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Отговорности за реагиране при PII инциденти и докладване на събития
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26;	Both	Supporting	Планиране, оценяване, реагиране, извлечени поуки и

	Control 5.27; Control 5.28			събиране на доказателства при инциденти
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Жизнен цикъл на процеса за управление на инциденти
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Политика, план, осведоменост, тестване и извлечени поуки при инциденти
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Операции по откриване, уведомяване, триаж, анализ, реагиране и докладване
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Очаквания за уведомяване и записи за нарушения при облачен обработващ лични данни
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Докладване на значими инциденти, когато е приложимо
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Управление, класификация и докладване на ИКТ инциденти, когато е приложимо

1. Обхват

1.1 Тази политика определя изискванията за идентифициране, докладване, триаж, оценяване, ограничаване, уведомяване, документиране, приключване и подобряване въз основа на PII инциденти и PII нарушения в обхвата на PIMS.

1.2 Тази политика се прилага за:

1.2.1 организацията, когато действа като администратор на PII;

1.2.2 организацията, когато действа като съвместен администратор и е необходима координация на отговорностите при нарушение;

1.2.3 организацията, когато действа като обработващ лични данни за PII;

1.2.4 организацията, когато действа като подизпълнител по обработване;

1.2.5 системи, приложения, услуги, процеси, доставчици, обработващи лични данни, подизпълнители по обработване и трети страни, които обработват, съхраняват, предават, поддържат, осъществяват достъп до или по друг начин влияят върху PII в обхвата на PIMS.

1.3 Тази политика използва REG10 - регистър на PII инциденти и нарушения като основен доказателствен обект за управление на PII инциденти и нарушения.

1.4 Тази политика използва поддържащи доказателствени обекти, както следва:

1.4.1 REG01 за обхвата на PIMS и контекста на приложимите заинтересовани страни, правните, договорните, секторните и клиентските изисквания за докладване.

1.4.2 REG02 за засегнатите дейности по обработване, категории PII, категории субекти на данни, цели и системи.

1.4.3 REG03 за Декларацията за приложимост и актуализации на приложимостта на контролите.

1.4.4 REG04 за връзка с риска за поверителността, DPIA и остатъчния риск.

1.4.5 REG08 за доказателства относно интерфейса за инциденти с обработващи лични данни, подизпълнители по обработване, клиенти, доставчици и трети страни.

1.4.6 REG09 за връзка с международни прехвърляния, когато инцидент засяга трансгранично обработване.

1.4.7 REG11 за доказателства за обучение, осведоменост и компетентност за реагиране при инциденти.

1.4.8 REG12 за доказателства за одит, несъответствие, коригиращо действие и подобрение.

1.5 Тази политика се основава на свързани PIMS политики за специализирани контроли:

1.5.1 PII03 урежда инвентара на обработването и записите за правно основание.

1.5.2 PII04 урежда контролите за уведомление за поверителност и прозрачност извън комуникациите, специфични за нарушения.

1.5.3 PII06 урежда исканията за упражняване на права от субекти на данни, възникнали преди, по време на или след инцидент.

1.5.4 PII07 урежда методологията за оценка на риска за поверителността и DPIA.

1.5.5 PII08 урежда контролите за поверителност още при проектиране и по подразбиране.

1.5.6 PII10 урежда контролите за съхранение, изтриване и унищожаване.

1.5.7 PII12 урежда контролите за взаимоотношенията с обработващи лични данни, подизпълнители по обработване, доставчици и трети страни във връзка с поверителността.

1.5.8 PII13 урежда механизмите за международно прехвърляне на PII и записите за риска при прехвърляне.

1.5.9 PII14 урежда превантивните и откриващите контроли за сигурност и достъп до PII.

1.5.10 PII16 урежда обучението, осведомеността и компетентността в областта на поверителността.

1.5.11 PII17 урежда документираната информация и управлението на доказателства.

1.5.12 PII18 урежда мониторинга, вътрешния одит, прегледа от ръководството, несъответствията, коригиращите действия и непрекъснатото подобрение.

1.6 За целите на тази политика:

1.6.1 „PII инцидент“ означава предполагаемо или потвърдено събитие, което е засегнало, може да е засегнало или разумно би могло да засегне поверителността, целостта, наличността, законосъобразното обработване или разрешеното боравене с PII.

1.6.2 „PII нарушение“ означава потвърден PII инцидент, включващ неоторизирано, незаконосъобразно, случайно или непреднамерено унищожаване, загуба, промяна, разкриване на, достъп до, неналичност на или компрометиране на PII.

1.6.3 „Оценка на нарушението“ означава документираната оценка дали даден PII инцидент представлява PII нарушение, кои PII и субекти на данни са засегнати, какви рискове могат да възникнат, какви уведомления или съобщения са необходими и какви мерки за отстраняване са нужни.

1.6.4 „Осведоменост“ означава моментът, в който организацията има разумна степен на сигурност, че е настъпил инцидент по сигурността или поверителността и PII е била или може да е била компрометирана.

1.6.5 „PII инцидент с високо въздействие“ означава PII инцидент, включващ високорисково обработване, специални категории или силно чувствителна PII, мащабна PII, уязвими лица, регулирани клиенти, въздействие в множество юрисдикции, съществено въздействие върху клиент, компрометиране на привилегирован достъп, публично излагане, ransomware, неналичност на услуга или значително оперативно или репутационно въздействие.

1.6.6 „Съществена промяна в информацията за инцидента“ означава нова или променена информация, която засяга обхвата, тежестта, категориите PII, въздействието върху субектите на данни, решението за уведомяване, въздействието върху клиент, първопричината, ограничаването, възстановяването, коригиращото действие или задълженията за външно докладване във връзка с инцидента.

2. Цел

2.1 Целта на тази политика е да гарантира, че PII инцидентите и нарушенията се обработват последователно, своевременно, законосъобразно, сигурно и с доказателства, подходящи за одит.

2.2 Тази политика подкрепя отчетността, като изисква PII инцидентите и нарушенията да се записват в REG10 и да се свързват със засегнатите записи за обработване, рисковете за поверителността, взаимоотношенията с обработващи лични данни и подизпълнители по обработване, записите за прехвърляне, коригиращите действия и записите за обучение, когато са задействани.

2.3 Тази политика гарантира, че задълженията на администратор, съвместен администратор, обработващ лични данни и подизпълнител по обработване се управляват чрез отделни правила за приложимост, като същевременно се поддържа един интегриран модел на доказателства за инциденти и нарушения.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 гарантира, че предполагаемите PII инциденти се докладват и записват своевременно;

3.1.2 гарантира, че PII инцидентите се подлагат на триаж и се класифицират по последователни критерии;

3.1.3 гарантира, че оценките на нарушенията отчитат засегнатите PII, субекти на данни, системи, дейности по обработване, обработващи лични данни, подизпълнители по обработване, прехвърляния, рискове и мерки за отстраняване;

3.1.4 гарантира, че решенията за уведомяване от администратора и за съобщаване до субектите на данни се документират;

3.1.5 гарантира, че уведомленията за нарушения от обработващи лични данни и подизпълнители по обработване до клиенти или страни нагоре по веригата се извършват без ненужно забавяне и съгласно приложимите споразумения;

3.1.6 гарантира, че доказателствата се запазват и защитават по време на обработването на инциденти;

3.1.7 гарантира, че ограничаването, отстраняването, възстановяването и валидирането се проследяват чрез REG10;

3.1.8 гарантира, че се оценяват тригерите за регулаторно, договорно, клиентско и секторно докладване, когато е приложимо;

3.1.9 гарантира, че извлечените поуки от инциденти водят до коригиращи действия и непрекъснато подобрение;

3.1.10 гарантира, че записите за инциденти и нарушения са налични за одит, преглед от ръководството, уверение за клиенти и регулаторен преглед, когато е приложимо.

4. Политически изисквания

4.1 Готовност за инциденти и приемане на сигнали

4.1.1 [Both] Privacy Lead / PIMS Manager MUST поддържа критерии за обработване на PII инциденти и нарушения в REG10 най-малко ежегодно и след всяка съществена промяна в обхвата на PIMS, правния контекст, договорните задължения или високорисковото обработване.

4.1.2 [All] Incident Response Coordinator MUST записва всеки докладван или открит предполагаем PII инцидент в REG10 в рамките на един работен ден от получаването или по-рано, когато може да бъде задействан приложим срок за уведомяване или клиентско докладване.

4.1.3 [Both] System Owner / Application Owner MUST запази съответните системни журнали, предупреждения, записи за достъп, доказателства за конфигурация и доказателства за възстановяване, свързани с REG10, когато предполагаем инцидент засяга система или приложение, обработващи PII.

4.1.4 [Both] Information Security Lead MUST извърши първоначален технически триаж на всяко събитие по сигурността, включващо PII, в рамките на 24 часа от откриването и да запише първоначалната тежест, засегнатите активи и статуса на ограничаване в REG10.

4.2 Класификация и оценка на нарушението

4.2.1 [Both] Incident Response Coordinator MUST класифицира всеки запис в REG10 като събитие без PII, предполагаем PII инцидент, потвърден PII инцидент или потвърдено PII нарушение в рамките на 24 часа от приемането или да актуализира записа в REG10 с причината, поради която класификацията остава неприключена.

4.2.2 [Both] Privacy Lead / PIMS Manager MUST идентифицира засегнатата дейност по обработване, категориите PII, категориите субекти на данни, системите, обработващите лични данни, подизпълнителите по обработване, местата на прехвърляне и рисковете за поверителността в REG02, REG04, REG08, REG09 и REG10, преди решението за уведомяване за нарушение да бъде финализирано.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor MUST оцени риска за засегнатите субекти на данни за всяко потвърдено или разумно предполагаемо PII нарушение и да запише препоръката за уведомяване, обосновката на риска и консултацията в REG10 преди вземането на решението за външно уведомяване.

4.2.4 [Processor] Privacy Lead / PIMS Manager MUST идентифицира засегнатия администратор или клиент и приложимите договорни изисквания за уведомяване веднага щом организацията узнае за PII нарушение, засягащо клиентска PII, и MUST запише резултата в REG08 и REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager MUST провери договорената отговорност при нарушение, водещата отговорност за комуникация и координационния механизъм преди всяко външно уведомяване или съобщаване от съвместен администратор и MUST запише решението в REG08 и REG10.

4.2.6 [Conditional] Privacy Lead / PIMS Manager MUST оцени приложимите правни, секторни, финансово-секторни, киберсигурностни, договорни, клиентски и за получатели на услуги тригери за докладване за всеки PII инцидент с високо въздействие и да запише резултата от приложимостта в REG01, REG08 и REG10.

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

9. Изключения

9.1.1 [Both] Privacy Lead / PIMS Manager MUST запише всяко изключение от тази политика в REG12 преди внедряването или в рамките на 24 часа след аварийно действие, когато предварителното одобрение не е било възможно.

9.1.2 [Both] Top Management MUST одобри всяко изключение, което съществено засяга сроковете за уведомяване за нарушение, публичната комуникация, ангажимент към клиент, запазването на доказателства или риска за субекти на данни преди приключването на инцидента, като доказателствата за одобрение се съхраняват в REG10 и REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUST документира консултация за всяко забавено уведомяване, решение за липса на уведомяване или изключителен подход към комуникацията преди приключване на инцидента, като консултацията се съхранява в REG10.

9.1.4 [Both] Vendor / Procurement Owner MUST запише изключения, инициирани от доставчик, обработващ лични данни, подизпълнител по обработване или клиент, които засягат реагирането при инцидент, в REG08 и REG12 в рамките на пет работни дни от идентифицирането на изключението.

10. Прилагане на политиката

10.1.1 [All] Process Owner / Business Owner MUST ескалира неизпълнение на задължението за докладване на предполагаем PII инцидент, запазване на доказателства, следване на възложени действия или сътрудничество при оценка на нарушение до Privacy Lead / PIMS Manager в рамките на два работни дни от откриването, като доказателствата се съхраняват в REG12.

10.1.2 [Both] Privacy Lead / PIMS Manager MUST запише несъответствие в REG12, когато нарушение на тази политика засяга приемането на инциденти, триажа, ограничаването, уведомяването, целостта на доказателствата, комуникацията или коригиращото действие.

10.1.3 [Both] Vendor / Procurement Owner MUST започне отстраняване от страна на доставчик или обработващ лични данни чрез REG08 и REG12 в рамките на пет работни дни, когато обработващ лични данни, подизпълнител по обработване, доставчик или друга трета страна не изпълни договорените задължения за инциденти или нарушения.

10.1.4 [Both] Top Management MUST прегледа съществени или повтарящи се несъответствия в управлението на инциденти при следващия планиран преглед от ръководството, като решенията и изисканите действия се съхраняват в REG12.

11. Преглед и поддръжка

11.1.1 [Both] Privacy Lead / PIMS Manager MUST преглежда тази политика най-малко ежегодно и да записва резултата от прегледа, необходимите промени и статуса на одобрение в REG12.

11.1.2 [Both] Incident Response Coordinator MUST задейства преглед на тази политика след инцидент в рамките на 30 календарни дни след приключването на всеки PII инцидент с високо въздействие или потвърдено PII нарушение, като доказателствата от прегледа се съхраняват в REG10 и REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager MUST прегледа тази политика в рамките на 30 календарни дни от узнаване за съществена промяна в приложимите правни, секторни, клиентски, договорни или свързани с обработващи лични данни, подизпълнители по обработване или прехвърляния изисквания за докладване на инциденти, като доказателствата от прегледа се съхраняват в REG01, REG08, REG09 и REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer MUST преглежда внедряването на тази политика най-малко ежегодно чрез програмата за вътрешен одит на PIMS, като одитните констатации и коригиращите действия се съхраняват в REG12.

11.1.5 [Both] Top Management MUST преглежда тенденциите при инцидентите, значимите нарушения, резултатността на уведомяването, просрочените коригиращи действия и ефективността на политиката по време на планиран преглед от ръководството, като резултатите се съхраняват в REG12.

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 PII06 - Политика за управление на права на субекти на данни

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

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

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

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

12.11 PII13 - Политика за международно прехвърляне на PII

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

12.13 PII16 - Политика за обучение, осведоменост и компетентност в областта на поверителността

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

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

13. Референтни стандарти и рамки

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].