					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII15-FS					Заглавие на документа: **Политика за управление на инциденти и нарушения на сигурността на личните данни във финансовия сектор**							
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 инциденти
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 на риска
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, законови, 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 клиент на обработващ лични данни и подпомагане на 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 инциденти между съвместни администратори
GDPR	Article 28	Both	Supporting	Съдействие от обработващ лични данни и договорни задължения на обработващия
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, мониторинг, сътрудничество и подпомагане като точка за контакт от DPO
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Процес за управление на ICT-свързани инциденти за финансови субекти в обхвата
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Критерии за класификация на ICT-свързани инциденти и значителни киберзаплахи
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Докладване на съществени ICT-свързани

				инциденти и уведомяване за значителни киберзаплахи
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Съдържание на докладването, срокове, образци и процедури
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Докладване на значими инциденти, когато е приложимо
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Принципи на информационната сигурност и съответствието в областта на поверителността
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Отговорности при реагиране на инциденти с PII и докладване на събития
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Планиране, оценяване, реагиране, извлечени поуки и 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 от публичен облачен обработващ лични данни

1. Обхват

1.1 Тази политика определя изискванията за идентифициране, докладване, триаж, класифициране, оценяване, ограничаване, уведомяване, документиране, приключване и подобряване въз основа на инциденти с лични данни и нарушения на сигурността на личните данни в обхвати на СУНЛИ във финансовия сектор.

1.2 **Указание за внедряване:** Тази политика е вариант за финансовия сектор, който заменя PII15. Тя не трябва да се внедрява едновременно с PII15 за един и същ обхват на СУНЛИ, бизнес единица, продукт, клиентска среда, регулирана услуга или доказателствена граница. Организациите трябва да изберат или PII15, или PII15-FS за същия обхват, за да избегнат дублирани задължения за управление на инциденти, дублирани регистри и дублирана работа по доказателства за одит.

1.3 Тази политика се прилага за:

1.3.1 организацията, когато действа като администратор в контекст на финансовия сектор;

1.3.2 организацията, когато действа като съвместен администратор, когато се изисква координация на отговорностите при инцидент или нарушение;

1.3.3 организацията, когато действа като обработващ лични данни за клиенти от финансовия сектор;

1.3.4 организацията, когато действа като подизпълнител по обработване за клиенти от финансовия сектор или за обработващи лични данни нагоре по веригата;

1.3.5 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 засягат PII в рамките на обхвата на СУНЛИ във финансовия сектор.

1.4 Тази политика използва REG10 - Регистър на инцидентите и нарушенията на сигурността на личните данни като основен доказателствен обект за управление на инциденти и нарушения на сигурността на личните данни във финансовия сектор.

1.5 Тази политика използва поддържащи доказателствени обекти, както следва:

1.5.1 REG01 за обхвата на СУНЛИ и приложимия контекст на заинтересованите страни, сектора, клиентите, договорите и докладването.

1.5.2 REG02 за засегнати дейности по обработване, категории PII, категории субекти на данни, цели, системи и услуги.

1.5.3 REG03 за Декларацията за приложимост и актуализации на приложимостта на контролите, включително замяната на PII15 с PII15-FS за същия обхват.

1.5.4 REG04 за връзката с риска за поверителността, DPIA, остатъчния риск и третирането на риска.

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

1.5.6 REG09 за връзката с международни прехвърляния, когато инцидент засяга трансгранично обработване.

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

1.5.8 REG12 за доказателства за одит, несъответствие, коригиращо действие, преглед от ръководството и подобрение.

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

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

1.6.2 PII04 урежда уведомлението за поверителност и контролите за прозрачност извън комуникациите, специфични за нарушения.

1.6.3 PII06 урежда исканията за упражняване на права на субекти на данни, които възникват преди, по време на или след инцидент.

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

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

1.6.6 PII10 урежда контролите за съхранение, изтриване и унищожаване.

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

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

1.6.9 PII14 урежда превантивните и откриващите контроли за сигурност на PII и контрол на достъпа.

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

1.6.11 PII17 урежда документираната информация и управлението на доказателства.

1.6.12 PII18 урежда мониторинга, вътрешния одит, прегледа от ръководството, несъответствието, коригиращото действие и непрекъснатото подобрение.

1.6.13 PII23 урежда контролите за облачни обработващи PII, когато задълженията на облачен обработващ лични данни са в обхвата.

1.7 За целите на тази политика:

1.7.1 „Инцидент с лични данни“ означава подозирано или потвърдено събитие, което е засегнало, може да е засегнало или основателно би могло да засегне поверителността, цялостта, наличността, законосъобразното обработване или разрешеното боравене с PII.

1.7.2 „Нарушение на сигурността на личните данни“ означава потвърден инцидент с лични данни, включващ неоторизирано, незаконосъобразно, случайно или непреднамерено унищожаване, загуба, изменение, разкриване, достъп, неналичност или компрометиране на PII.

1.7.3 „Инцидент с лични данни във финансовия сектор“ означава инцидент с лични данни, който засяга, може да засегне или е основателно свързан с регулирани финансови услуги, клиенти от финансовия сектор, финансови контрагенти, финансови транзакции, финансови операции или обработване на PII във финансовия сектор.

1.7.4 „Съществен инцидент във финансовия сектор“ означава инцидент с лични данни във финансовия сектор или свързан ICT инцидент, който отговаря на документирани критерии за същественост или докладване в REG10.

1.7.5 „Значителна киберзаплаха“ означава киберзаплаха, записана в REG10, която би могла съществено да засегне финансови услуги, обработване на PII, клиенти, контрагенти или операции в обхвата.

1.7.6 „Оценка на нарушението“ означава документирана оценка дали инцидент с лични данни е нарушение на сигурността на личните данни, какви PII и субекти на данни са засегнати, какви рискове могат да възникнат, какви уведомления или комуникации са необходими и какво коригиращо действие е нужно.

1.7.7 „Узнаване“ означава моментът, в който организацията има разумна степен на сигурност, че е настъпил инцидент по сигурността или поверителността и PII са били или може да са били компрометирани.

1.7.8 „Инцидент с лични данни с високо въздействие във финансовия сектор“ означава инцидент с лични данни, включващ високорисково обработване, специални категории или силно чувствителни PII, PII в голям мащаб, уязвими лица, регулирани клиенти, съществено прекъсване на услуга, финансови контрагенти, финансови транзакции, въздействие в множество юрисдикции, компрометиране на привилегирован достъп, публично излагане, ransomware, неналичност на услуга или значимо оперативно, клиентско, финансово или репутационно въздействие.

1.7.9 „Съществена промяна в информацията за инцидента“ означава нова или променена информация, засягаща обхвата на инцидента, тежестта, категориите PII, въздействието върху субектите на данни, въздействието върху услугите, класификацията за финансовия сектор, решението за уведомяване, въздействието върху клиента, първопричината, ограничаването, възстановяването, коригиращото действие или задълженията за външно докладване.

2. Цел

2.1 Целта на тази политика е да гарантира, че инцидентите с лични данни и нарушенията на сигурността на личните данни във финансовия сектор се обработват последователно, своевременно, законосъобразно, сигурно и с доказателства, готови за одит.

2.2 Тази политика подпомага отчетността, като изисква инцидентите с лични данни и нарушенията на сигурността на личните данни във финансовия сектор да се записват в REG10 и да се свързват със засегнати записи за обработване, рискове за поверителността, взаимоотношения с обработващи лични данни и подизпълнители по обработване, записи за прехвърляния, коригиращи действия, записи за обучение, решения за докладване във финансовия сектор и доказателства за преглед от ръководството, когато са задействани.

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

3. Цели

3.1 Целите на тази политика са да:

3.1.1 гарантира, че подозирани инциденти с лични данни във финансовия сектор се докладват и записват своевременно;

3.1.2 гарантира, че инцидентите с лични данни във финансовия сектор преминават триаж и класификация чрез последователни критерии за поверителност, сигурност, операции и секторен контекст;

3.1.3 гарантира, че оценките на нарушенията отчитат засегнатите PII, субекти на данни, системи, услуги, дейности по обработване, обработващи лични данни, подизпълнители по обработване, прехвърляния, рискове, клиенти, контрагенти и коригиращи действия;

3.1.4 гарантира, че решенията за уведомяване от администратора и за комуникация със субекти на данни се документират;

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

3.1.6 гарантира, че критериите за задействане на докладване във финансовия сектор се оценяват, документират и проследяват, когато е приложимо;

3.1.7 гарантира, че доказателствата се запазват и защитават при обработване на инциденти;

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

3.1.9 гарантира, че значителните киберзаплахи и съществените инциденти във финансовия сектор се насочват към подходящи работни потоци за решения и докладване;

3.1.10 гарантира, че извлечените поуки от инциденти водят до коригиращи действия, обучение, подобрение на контролите и преглед от ръководството;

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

3.1.12 гарантира, че PII15-FS заменя PII15 за същия обхват във финансовия сектор и не дублира работата по доказателства по PII15.

4. Изисквания на политиката

4.1 Активиране на варианта, готовност и приемане на сигнали

4.1.1 [Conditional] Privacy Lead / PIMS Manager трябва да документира активирането на PII15-FS в REG01 и REG03, преди тази политика да се използва за обхват на СУНЛИ във финансовия сектор.

4.1.2 [Conditional] Privacy Lead / PIMS Manager трябва да документира в REG03 и REG12, че PII15 не е внедрена едновременно за същия обхват на СУНЛИ във финансовия сектор, преди PII15-FS да бъде одобрена.

4.1.3 [All] Incident Response Coordinator трябва да запише всеки докладван или открит подозиран инцидент с лични данни във финансовия сектор в REG10 в рамките на един работен ден от получаването или по-рано, когато може да бъде задействан приложим срок за уведомяване, клиентски срок или срок за докладване.

4.1.4 [Conditional] Privacy Lead / PIMS Manager трябва да поддържа критерии за обработване на инциденти и нарушения на сигурността на личните данни във финансовия сектор в REG10 най-малко ежегодно и след всяка съществена промяна в обхвата на СУНЛИ, правния контекст, задълженията към клиенти, договорните задължения, секторния контекст на докладване или високорисковото обработване.

4.1.5 [Both] Information Security Lead трябва да потвърди изискванията за запазване на доказателства за инциденти в REG10 в рамките на 24 часа след като подозиран инцидент засегне система, услуга или приложение, обработващи PII.

4.1.6 [Conditional] Vendor / Procurement Owner трябва да поддържа изискванията за контакти при инциденти с трети страни във финансовия сектор и за маршрутизиране на доказателства в REG08 преди въвеждане и най-малко ежегодно за обработващи лични данни, подизпълнители по обработване, доставчици и външно възложени доставчици на докладване в обхвата.

4.2 Класификация и оценка на нарушението

4.2.1 [All] Incident Response Coordinator трябва да класифицира всеки запис в REG10 в рамките на 24 часа от приемането като събитие без PII, подозиран инцидент с лични данни, потвърден инцидент с лични данни, потвърдено нарушение на сигурността на личните данни, инцидент с лични данни във финансовия сектор, съществен инцидент във финансовия сектор, значителна киберзаплаха или запис с предстояща класификация.

4.2.2 [Conditional] Information Security Lead трябва да оцени засегнатите услуги, клиенти, контрагенти, транзакции, прекъсване на услуги, географско разпространение, загуба на данни, критичност на услугите и икономическо въздействие в REG10, когато инцидент с лични данни може да засегне услуги или операции във финансовия сектор.

4.2.3 [Both] Privacy Lead / PIMS Manager трябва да 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.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor трябва да оцени риска за засегнатите субекти на данни за всяко потвърдено или основателно подозирано нарушение на сигурността на личните данни и да запише препоръката за уведомяване, обосновката на риска и консултацията в REG10, преди да бъде взето решението за външно уведомяване.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager трябва да запише разпределението на отговорностите при инцидент между съвместни администратори в REG08 и REG10 в рамките на 24 часа след установяване на споделена отговорност за подозирано или потвърдено нарушение на сигурността на личните данни.

4.2.6 [Processor] Privacy Lead / PIMS Manager трябва да оцени нарежданията на клиента, договорните задължения за уведомяване и задълженията за сътрудничество в REG08 и REG10 в рамките на 24 часа след като подозирано или потвърдено нарушение на сигурността на личните данни засегне обработване, извършвано като обработващ лични данни.

4.2.7 [Subprocessor] Vendor / Procurement Owner трябва да идентифицира веригата за уведомяване нагоре по веригата и необходимото маршрутизиране на доказателства в REG08 и REG10 в рамките на 24 часа след като подозиран или потвърден инцидент с лични данни засегне обработване, извършвано като подизпълнител по обработване.

[... 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] Privacy Lead / PIMS Manager трябва да запише всяко изключение от тази политика в REG12 преди внедряване или в рамките на 24 часа след аварийно действие, когато предварително одобрение не е било осъществимо.

9.1.2 [Conditional] Top Management трябва да одобри всяко изключение, което съществено засяга сроковете за уведомяване за нарушение, сроковете за докладване във финансовия сектор, публична комуникация, ангажимент към клиент, запазване на доказателства или риск за субектите на данни, преди инцидентът да бъде приключен, като доказателствата за одобрение се съхраняват в REG10 и REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor трябва да документира консултация за всяко забавено уведомяване, решение за неуведомяване, изключение при докладване или изключителен подход към комуникация преди приключване на инцидента, като консултацията се съхранява в REG10.

9.1.4 [Both] Vendor / Procurement Owner трябва да запише изключения на доставчик, обработващ лични данни, подизпълнител по обработване, клиент или външно възложен доставчик, които засягат реагирането при инциденти във финансовия сектор, в REG08 и REG12 в рамките на пет работни дни след идентифициране на изключението.

9.1.5 [All] Privacy Lead / PIMS Manager трябва да преглежда отворените изключения от тази политика най-малко месечно до приключването им, като статусът на прегледа се съхранява в REG12.

10. Прилагане на политиката

10.1.1 [All] Process Owner / Business Owner трябва да ескалира неизпълнение на задължение за докладване на подозиран инцидент с лични данни във финансовия сектор, запазване на доказателства, следване на възложени действия или сътрудничество при оценка на нарушение към Privacy Lead / PIMS Manager в рамките на два работни дни след откриването, като доказателствата се съхраняват в REG12.

10.1.2 [Both] Incident Response Coordinator трябва да ескалира късно докладване, пропусната класификация, липсващи доказателства, пропусната ескалация или просрочено действие по ограничаване към Privacy Lead / PIMS Manager в рамките на един работен ден след идентифициране на проблема, като доказателствата се съхраняват в REG10 и REG12.

10.1.3 [Both] Privacy Lead / PIMS Manager трябва да запише несъответствие в REG12, когато нарушение на тази политика засяга приемането на инцидент, триажа, ограничаването, уведомяването, докладването, целостта на доказателствата, комуникацията или коригиращото действие.

10.1.4 [Both] Vendor / Procurement Owner трябва да започне отстраняване от страна на доставчик, обработващ лични данни, подизпълнител по обработване или външно възложен доставчик чрез REG08 и REG12 в рамките на пет работни дни, когато трета страна не изпълни договорените задължения за инцидент, нарушение, доказателства или докладване.

10.1.5 [Conditional] Top Management трябва да прегледа съществени или повтарящи се несъответствия с PII15-FS на следващия планиран преглед от ръководството, като решенията и необходимите действия се съхраняват в REG12.

10.1.6 [All] Privacy Lead / PIMS Manager трябва да задейства коригиращо обучение в REG11 в рамките на 30 календарни дни, когато несъответствие с политиката включва осведоменост по роля, късно докладване, неизпълнена ескалация, неправилно обработване на доказателства или неуспешна комуникация.

11. Преглед и поддръжка

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

11.1.2 [Conditional] Incident Response Coordinator трябва да задейства слединцидентен преглед на тази политика в рамките на 30 календарни дни след приключване на всеки инцидент с лични данни с високо въздействие във финансовия сектор, потвърдено нарушение на сигурността на личните данни, съществен инцидент във финансовия сектор или значителна киберзаплаха, като доказателствата от прегледа се съхраняват в REG10 и REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager трябва да прегледа тази политика в рамките на 30 календарни дни след узнаване за съществена промяна в правни, секторни, клиентски, договорни, свързани с обработващ лични данни, подизпълнител по обработване, образец за докладване, срок за докладване или свързани с прехвърляне 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 трябва да 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 [Conditional] Top Management трябва да преглежда тенденциите при инциденти, значимите нарушения, резултатността на докладването, просрочените коригиращи действия и ефективността на политиката по време на планиран преглед от ръководството, като резултатите се съхраняват в REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager трябва да преглежда заместващата връзка между PII15-FS и PII15 най-малко ежегодно и след всяка промяна в обхвата на PIMS, за да провери, че двете политики не са внедрени за един и същ обхват във финансовия сектор, като доказателствата от прегледа се съхраняват в REG03 и REG12.

12. Свързани политики

12.1 Тази политика следва да се чете заедно със:

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

12.1.2 PII02 - Политика за роли, отговорности и отчетност в областта на поверителността

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

12.1.4 PII04 - Политика за уведомление за поверителност и прозрачност

12.1.5 PII06 - Политика за управление на права на субекти на данни

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

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

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

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

12.1.10 PII13 - Политика за международно прехвърляне на PII

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

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

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

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

12.1.15 PII23 - Политика за облачен обработващ PII, когато задълженията на облачен обработващ лични данни във финансовия сектор са в обхвата

12.2 PII15 - Политика за управление на инциденти и нарушения на сигурността на личните данни е базовата политика за инциденти и нарушения. PII15-FS е вариант за финансовия сектор, който заменя PII15. PII15 и PII15-FS не трябва да се внедряват едновременно за един и същ обхват на СУНЛИ, бизнес единица, продукт, клиентска среда, регулирана услуга или доказателствена граница.

13. Референтни стандарти и рамки

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 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; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 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 [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].