					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P17					Заглавие на документа: **Политика за защита на данните и поверителност**							
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**

Съгласуваност с приложимите стандарти и регулации

Стандарт/регулация	**Клауза/член**	**Коментар**
ISO/IEC 27001:2022	Клаузи 5.1, 6.1.3, 8.1, 10	Приложими общи, технически и свързани с непрекъснатото подобрение контроли за защита на данните
ISO/IEC 27002:2022	Контроли 5.34, 8.10, 8.11, 8.12	Контроли за обработване на PII, съхранение, изтриване, анонимизиране и права на субектите на данни
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Изисквания за управление, риск, управление на достъпа, журнализиране, реагиране при нарушения и програма за поверителност
GDPR на ЕС	Членове 5, 6, 12–23, 25, 28, 30, 32–34; Съображение 78	Всички основни изисквания за поверителност, отчетност, права на субектите, DSR, нарушения, принципи за защита още при проектиране и по подразбиране
Директива NIS2 на ЕС	Член 21(2)(e), (f)	Контроли за сигурност, базирани на риска, за съществени и важни субекти
DORA на ЕС	Членове 6(2)(d), 11(1)(c), 15(1), 17	Управление, риск от трети страни и срокове за сигурно обработване
COBIT 2019	APO12, DSS01, DSS05, MEA	Управление на риска, сигурни операции, надзор върху съответствието

1. Цел

1.1 Настоящата политика установява задължителни организационни принципи и технически изисквания за защитата на личните данни и за прилагането на защитата на данните още при проектиране във всички среди.

1.2 Тя формализира отговорностите на организацията съгласно международните стандарти и регулаторните рамки, като гарантира, че личните данни се събират, обработват, съхраняват, споделят и унищожават законосъобразно, сигурно и прозрачно.

1.3 Настоящата политика също така утвърждава съответствието с приложимите закони и рамки в областта на поверителността, включително Общия регламент относно защитата на данните (GDPR), Директива NIS2 на ЕС, Регламента на ЕС за цифрова оперативна устойчивост (DORA), ISO/IEC 27001:2022 и COBIT 2019.

2. Обхват

2.1 Настоящата политика се прилага за всички организационни единици, служители и системи, участващи в обработването на лични данни, включително:

2.1.1 Служители, външни изпълнители, консултанти и външни доставчици на услуги.

2.1.2 Данни, събрани от вътрешни и външни източници във всички бизнес функции.

2.1.3 Физически и цифрови носители, включително облачни услуги, SaaS платформи, мобилни устройства и записи на хартиен носител.

2.1.4 Всички среди, включително продукционни, развойни, тестови системи и системи за резервни копия, в които може да се съдържат лични данни.

2.2 Политиката обхваща всички дейности по обработване, регулирани от приложимите закони и стандарти в областта на поверителността, включително, но не само:

2.2.1 Събиране, съхранение, използване, предаване и унищожаване на лични данни.

2.2.2 Гарантиране на правата на субектите на данни, документиране на правното основание и управление на съгласието.

2.2.3 Трансгранични прехвърляния, уведомяване при нарушения и споделяне на данни с трети страни.

2.2.4 Защита на данните още при проектиране и прилагане на поверителност по подразбиране в системите и процесите.

3. Цели

3.1 Да се осигури законосъобразно, прозрачно и отчетно обработване на лични данни в съответствие с ISO/IEC 27001:2022 и свързаните правни изисквания.

3.2 Да се внедрят принципите за защита на данните още при проектиране и по подразбиране във всички информационни системи, услуги и бизнес процеси.

3.3 Да се прилагат технически и организационни мерки (TOMs), които защитават поверителността, целостта и наличността на личните данни през целия им жизнен цикъл.

3.4 Да се определят роли по управление и структури на отчетност за защита на данните, включително отговорностите на длъжностното лице по защита на данните (DPO), функцията по информационна сигурност, правния отдел и собствениците на данни.

3.5 Да се осигури пълно съответствие с членове 5, 6, 25, 30 и 32 от GDPR, както и с изискванията за намаляване на риска и устойчивост съгласно NIS2 и DORA.

3.6 Да се гарантират правата на субектите на данни, включително достъп, коригиране, изтриване, ограничаване, преносимост, възражение и защита срещу автоматизирано вземане на решения.

3.7 Да се смекчават регулаторните, репутационните, правните и оперативните рискове, произтичащи от неоторизиран достъп, неправомерно използване или загуба на лични данни.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Осигурява стратегически надзор и разпределя достатъчни ресурси в подкрепа на програмата за поверителност.

4.1.2 Одобрява настоящата политика и гарантира нейното прилагане в цялата организация.

4.2 Длъжностно лице по защита на данните (DPO)

4.2.1 Действа независимо при надзора върху съответствието с регулациите за защита на данните.

4.2.2 Поддържа Регистър на дейностите по обработване (RoPA) съгласно член 30 от GDPR.

4.2.3 Ръководи взаимодействието с регулаторните органи, извършва оценки на въздействието върху защитата на данните (DPIA) и управлява процесите по уведомяване при нарушения.

4.2.4 Преглежда изключенията, свързани с поверителността, и поддържа Регистър на изключенията за поверителност.

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

9. Изисквания за преглед и актуализация

9.1 Настоящата политика трябва да се преглежда най-малко веднъж годишно или по-рано при следните условия:

9.1.1 Съществени правни или регулаторни актуализации (напр. изменения в GDPR, срокове по DORA)

9.1.2 Нови системи или дейности по обработване, включващи лични данни

9.1.3 Одитни констатации от вътрешен одит, които показват пропуски в политиката

9.1.4 Съществени инциденти, свързани с нарушения, или обратна връзка от надзорен орган

9.2 Отговорности по прегледа

9.2.1 DPO трябва да инициира прегледа на политиката, като координира с Правния отдел, управлението на риска, функцията по информационна сигурност и Изпълнителното ръководство.

9.2.2 Всички актуализации трябва да бъдат записани в Регистъра за контрол на документите на СУИС и разпространени до засегнатите заинтересовани страни.

9.3 Контрол на промените

9.3.1 Всяка редакция на настоящата политика трябва да бъде официално одобрена от Изпълнителното ръководство.

9.3.2 Остарелите версии трябва да се архивират сигурно, а актуализираната версия трябва да включва документирана история на промените.

10. Свързани политики и връзки

10.1 P1 – Политика за информационна сигурност. Определя общите принципи за управление на сигурността, върху които се основава настоящата политика за поверителност. P1 подпомага поверителността, целостта и наличността на личните данни във всички системи и услуги.

10.2 P6 – Политика за управление на риска. Определя методологията на организацията за третиране на риска, която е съществена за оценяване на рисковете за поверителността, процесите по DPIA и оценките на остатъчния риск, изисквани по GDPR и ISO/IEC 27001, клауза 6.1.3.

10.3 P13 – Политика за класификация и етикетиране на данни. Определя насоките за категоризиране на лични и чувствителни данни, което формира основата за прилагане на подходящи контроли за поверителност, включително налагане на срокове за съхранение, ограничаване на достъпа и сигурно унищожаване.

10.4 P14 – Политика за съхранение и унищожаване на данни. Пряко подпомага изискванията за поверителност по членове 5(1)(e) и 17 от GDPR, като гарантира, че личните данни се съхраняват само доколкото е необходимо и се унищожават сигурно в съответствие с правните задължения.

10.5 P16 – Политика за маскиране на данни и псевдонимизация. Установява контроли за намаляване на възможността за идентифициране на лични данни чрез технически мерки като токенизация, динамично маскиране и псевдонимизация, като по този начин прилага член 32 от GDPR и Контрол 5.34 от ISO/IEC 27002.

10.6 P30 – Политика за реагиране при инциденти. Определя задължителните протоколи за реагиране при нарушения, които се интегрират с обработването на нарушения, свързани с поверителността, и със сроковете за уведомяване, изисквани по членове 33 и 34 от GDPR.

10.7 P33 – Политика за одит и мониторинг на съответствието. Налага планирани оценки на ефективността на програмата за поверителност, прилагането на политиката и проследяването

на коригиращи действия в организационните единици и при трети страни, обработващи лични данни.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 5.1 – Лидерство и ангажираност: Установява отговорност на изпълнителното ниво за защитата на личните данни и прилагането на принципите за поверителност.

11.1.2 Клауза 6.1.3 – Третиране на риска за информационната сигурност: Подпомага идентифицирането, оценяването и третирането на рисковете за поверителността чрез DPIA и изключения.

11.1.3 Клауза 8.1 – Оперативно планиране и контрол: Изисква технически и процедурни предпазни мерки, за да се гарантира сигурното обработване на лични данни.

11.1.4 Клауза 10.1 – Непрекъснато подобрение: Изисква периодична оценка и адаптиране на програмата за поверителност.

11.2 ISO/IEC 27002:2022, Контроли 5.34, 8.10, 8.11, 8.12: Предоставя насоки за обработването на PII, прилагането на срокове за съхранение, изтриване, анонимизиране и прозрачност по отношение на правата на субектите.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: Определят отговорности по управление, роли, отчетност и обучение по поверителност.

11.3.2 PL-2, PL-8: Изискват интегриране на контролите за поверителност в жизнения цикъл на системите и корпоративната архитектура.

11.3.3 AC-2, AC-6: Налагат минимално необходим достъп и управление на акаунти за защита на личните данни.

11.3.4 AU-2, AU-6, AU-9: Изискват журнализиране, проследимост и цялост на одита за достъпа до лични данни.

11.3.5 IR-4, IR-5, IR-6: Определят структурирани процеси за откриване, анализ и докладване на нарушения, свързани с поверителността.

11.3.6 PM-1, PM-21, PM-23: Установяват цялостна програма за поверителност, съгласувана със стратегическия риск и целите за управление на данните.

11.4 GDPR на ЕС (2016/679)

11.4.1 Членове 5, 6, 12–23, 25, 28, 30, 32–34: Регулират законосъобразното обработване, ограничаването на целите, правата на субектите на данни, отчетността, защитата на данните още при проектиране и по подразбиране, задълженията на трети страни и управлението на нарушения.

11.4.2 Съображение 78: Утвърждава принципите за защита на данните още при проектиране.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Член 21(2)(e) и (f): Изисква внедряване на контроли за сигурност, базирани на риска, и защита на личните данни в обхвата на съществени и важни субекти.

11.6 DORA на ЕС (2022/2554)

11.6.1 Член 6(2)(d): Налага вътрешно управление на ИКТ риска, свързан с обработването на данни.

11.6.2 Член 11(1)(c): Изисква надзор върху риска от трети страни за услуги, свързани с данни.

11.6.3 Членове 15(1) и 17: Изискват сигурно обработване на данни от доставчици на услуги и своевременно уведомяване на надзорните органи след инциденти, свързани с ИКТ.

11.7 COBIT 2019

11.7.1 APO12 – Управление на риска: Интегрира риска за поверителността в по-широкия надзор върху корпоративния риск.

11.7.2 DSS01 – Управлявани операции и DSS05: Осигуряват сигурни операции, включително контрол на достъпа, срокове за съхранение и целостта на системите.

11.7.3 MEA03 – Непрекъснат мониторинг на съответствието: Изисква текущ преглед на статуса на съответствието спрямо регулаторните и основаните на политики задължения за поверителност.