					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P37					Заглавие на документа: **Политика за правно и регулаторно съответствие**							
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**

1. Цел

1.1 Настоящата политика установява задължителна рамка за идентифициране, управление и спазване на всички правни, регулаторни и договорни задължения, приложими към информационната сигурност, защитата на данните и оперативните функции на организацията.

1.2 Целта е да се предотврати несъответствие, което може да доведе до глоби, правна отговорност, прекъсване на дейността, репутационни щети или регулаторни принудителни мерки.

1.3 Настоящата политика подпомага интегрирането на изискванията за съответствие в управлението, процесите по управление на риска, оперативните процеси, жизнените цикли на проектите и проектирането на системи.

1.4 Тя гарантира, че всички приложими задължения — в различни юрисдикции, отрасли и регулаторни обхвати — са ясно документирани, оценени, наблюдавани и прилагани в рамките на организацията.

2. Обхват

2.1 Настоящата политика се прилага за всички отдели, функции, бизнес звена и лица, действащи от името на организацията, включително:

2.1.1 Постоянни и временни служители

2.1.2 Външни изпълнители, консултанти и стажанти

2.1.3 Доставчици — трети страни, обработващи лични данни, или партньори, които обработват данни на организацията, използват нейните системи или изпълняват нейни регулаторни задължения

2.1.4 Всеки бизнес процес, проект или инициатива, подлежащи на правен или регулаторен надзор

2.2 Областите на съответствие, обхванати от тази политика, включват, но не се ограничават до:

2.2.1 Задължения в областта на информационната сигурност и киберсигурността (напр. ISO/IEC 27001, NIS2, DORA)

2.2.2 Законодателство в областта на защитата на данните и поверителността (напр. GDPR, секторно законодателство в областта на поверителността)

2.2.3 Секторни регулации (напр. финансов сектор, здравеопазване, автомобилна индустрия, отбрана)

2.2.4 Договорни задължения, произтичащи от споразумения за неразкриване на информация (NDA), споразумения за ниво на услугата (SLA) или споразумения за обработване на лични данни

2.2.5 Правни изисквания, свързани с докладване на инциденти, взаимодействие с правоохранителните органи и международен трансфер на данни

3. Цели

3.1 Да се гарантира, че всички приложими закони, регулации, стандарти и договорни задължения са идентифицирани, документирани, тълкувани и прилагани в цялата организация.

3.2 Да се интегрират правните и регулаторните изисквания в СУИС на организацията, процесите по управление на риска, договорите с доставчици и проектирането на продукти и услуги.

3.3 Да се осигури механизъм за проактивно наблюдение на регулаторните промени и своевременно актуализиране на контролите и документацията.

3.4 Да се определят ясни отговорности за надзор върху съответствието, ескалация на нарушения, управление на изключения и външно докладване.

3.5 Да се осигури проследимост за одит и защита на правната и регулаторната позиция на организацията при проверки, разследвания или сертификационни прегледи.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Носи стратегическа отговорност за съответствието с правните и регулаторните изисквания в рамките на цялата организация.

4.1.2 Преглежда и одобрява решения по съответствие с висок риск, включително приемане на риск и правни спорове.

4.2 Длъжностно лице по съответствието / Главен юрисконсулт / Юрисконсулт

4.2.1 Поддържа Регистър на задълженията по съответствие, който съдържа всички приложими закони, стандарти, сертификационни изисквания и договорни клаузи.

4.2.2 Извършва оценки на правното въздействие за нови услуги, пазари или потоци от данни.

4.2.3 Предоставя официално тълкуване на закони и стандарти.

[... 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 Годишен преглед на политиката

9.1.1 Настоящата политика трябва да се преглежда най-малко веднъж на календарна година, за да:

9.1.1.1 Осигури непрекъснато съответствие с актуализирани закони, отраслови стандарти и регулаторни рамки

9.1.1.2 Валидира оперативната ефективност въз основа на одитни констатации и историята на инцидентите

9.1.1.3 Отрази организационни промени (напр. нови юрисдикции, системи или бизнес направления)

9.2 Прегледи при настъпване на събитие

9.2.1 Междинни прегледи трябва да бъдат инициирани, когато:

9.2.2 Влезе в сила или бъде актуализирано ново правно или регулаторно изискване

9.2.3 Инцидент по съответствието или одит разкрие слабости в политиката

9.2.4 Организацията навлезе на нов пазар или започне нова услуга, подчинени на отделни рамки за съответствие

9.2.5 Тенденциите в правоприлагането или указанията на регулаторите показват промени в рисковия профил

9.3 Собственост и одобрение

9.3.1 Правният отдел и длъжностното лице по съответствието носят съвместна отговорност за координирането на процеса по преглед.

9.3.2 Окончателните редакции на политиката трябва да бъдат одобрени от Изпълнителното ръководство и регистрирани в Регистъра на промените в политиките, заедно със свързаните препратки за контрол на промените и планове за комуникация.

9.4 Управление на версиите и комуникация

9.4.1 Всяка актуализирана версия на настоящата политика трябва:

9.4.1.1 Да включва обобщение на основните промени

9.4.1.2 Да бъде разпространена повторно чрез официални канали (напр. портал за политики, LMS, вътрешни бюлетини)

9.4.1.3 Да изисква потвърждение от засегнатия персонал, особено от лица с роли в правните въпроси, операциите, сигурността и управлението на доставчици

10. Свързани политики и връзки

10.1 Настоящата политика се прилага съвместно със следните политики в рамките на СУИС на организацията и ги допълва:

10.1.1 P1 – Политика за информационна сигурност: Установява основните принципи за управление, които гарантират, че всички политики по информационна сигурност — включително тези за съответствие — са съгласувани със стратегическите бизнес и регулаторни изисквания.

10.1.2 P2 – Политика за роли и отговорности в управлението: Определя правомощията за вземане на решения, включително правните и съответните роли, отговорни за регулаторния надзор и отчетността.

10.1.3 P6 – Политика за управление на риска: Подпомага оценката, собствеността и смекчаването на правните и регулаторните рискове, свързани със съответствието, в рамките на цялата организация.

10.1.4 P8 – Политика за осведоменост и обучение по информационна сигурност: Гарантира, че целият персонал е информиран за своите задължения по съответствие и получава обучение, съобразено с ролята му.

10.1.5 P12 – Политика за управление на активите: Подкрепя правните задължения за управление и защита на регулирани или договорни активи, включително такива, които съдържат лични данни и са част от критична инфраструктура.

10.1.6 P30 – Политика за реагиране при инциденти: Управлява задължителните правни уведомления (напр. член 33 от GDPR) и процедурите за ескалация при нарушение на съответствието или регулаторно събитие.

10.1.7 P33 – Политика за одит и мониторинг на съответствието: Осигурява структурирани дейности по осигуряване, включително тестване на контролите и събиране на доказателства, необходими за вътрешна и външна проверка на съответствието.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 4.2 – Разбиране на нуждите и очакванията на заинтересованите страни: Изисква идентифициране и интегриране на правните и регулаторните изисквания в СУИС.

11.1.2 Клауза 5.1 – Лидерство и ангажираност: Налага отговорност на изпълнителното ръководство за установяване и поддържане на правното съответствие в цялата организация.

11.1.3 Клауза 5.3 – Организационни роли, отговорности и правомощия: Осигурява яснота на ролите за правен надзор и регулаторно съответствие.

11.1.4 Приложение A, Контрол 5.36 – Съответствие с правни и договорни изисквания: Установява изискването за идентифициране и изпълнение на задълженията, произтичащи от закони, регулации и договори.

11.2 ISO/IEC 27002

11.2.1 Контрол 5.36: Дава насоки за прилагане при поддържане на регистър на задълженията по съответствие, валидиране на регулаторните изисквания и осигуряване на структурирано съхранение на доказателства.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Политика и процедури за планиране на сигурността: Изисква изискванията за съответствие да бъдат вградени в структурите за управление и документацията.

11.3.2 PM-1 – План на програмата по информационна сигурност: Изисква регулаторните контроли да бъдат компонент от по-широката програма по сигурност.

11.3.3 CA-7 – Непрекъснат мониторинг: Подкрепя надзора върху ефективността на контролите за изпълнение на правните изисквания и изискванията на политиките.

11.3.4 AU-9 – Защита на одитната информация: Осигурява защита на журналите и записите за одит по съответствието и тяхната наличност за проверка.

11.4 GDPR на ЕС (2016/679)

11.4.1 Член 5 – Принципи, свързани с обработването: Изисква законосъобразно обработване, прозрачност и принцип на отчетност.

11.4.2 Член 6 – Законосъобразност на обработването: Изисква подходящи правни основания за всички дейности по обработване на данни.

11.4.3 Член 24 – Отговорност на администратора: Установява пряка отчетност за гарантиране на регулаторно съответствие.

11.4.4 Член 32 – Сигурност на обработването: Изисква прилагане на подходящи технически и организационни контроли.

11.4.5 Член 33 – Уведомяване при нарушение: Изисква нарушенията на сигурността на личните данни да бъдат докладвани на компетентните органи в срок до 72 часа.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Членове 20–21: Изискват съществените и важните субекти да прилагат документирано управление, стратегии за правно съответствие и непрекъснат преглед на правните рискове.

11.6 DORA на ЕС (2022/2554)

11.6.1 Член 5(2) – Рамка за управление на риска в областта на ИКТ: Изисква интегриране на правното съответствие в по-широките функции по управление на риска и надзор.

11.6.2 Член 19 – Риск от трети страни в областта на ИКТ: Налага специфични правни изисквания за управление на договорните и регулаторните задължения, свързани с външни доставчици и платформи.

11.7 COBIT 2019

11.7.1 APO12 – Управление на риска: Включва правното и регулаторното съответствие като критични компоненти на управлението на корпоративния риск.

11.7.2 MEA03 – Мониторинг на съответствието с външни изисквания: Определя текущ мониторинг, управление на изключения и готовност за одит за всички форми на регулаторни задължения.