					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P37S					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**

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Контрол 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
GDPR на ЕС	Членове 5, 6, 32, 33	
NIS2 на ЕС	Членове 21(2)(a), 21(2)(f), 23	
DORA на ЕС	Членове 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Цел

1.1 Настоящата политика определя подхода на организацията за идентифициране, спазване и доказване на съответствието с правни, регулаторни и договорни задължения.

1.2 Тя определя ясни отговорности и практически стъпки, които подпомагат дружеството при изпълнение на задълженията му по съответствие, включително по отношение на законодателството за защита на данните, рамките за киберсигурност, клиентските споразумения и стандартите за сертификация.

1.3 Тя гарантира, че дори при липса на отделен екип по съответствие дружеството може да поддържа правно издържани операции, да реагира адекватно при инциденти и да запазва готовност за одит.

1.4 Тази политика е съществена за постигане на сертификация по ISO/IEC 27001:2022 и за изпълнение на външните изисквания на клиенти, регулатори и партньори.

2. Обхват

2.1 Тази политика се прилага за:

2.1.1 всички служители, външни изпълнители, фрийлансъри и доставчици от трети страни;

2.1.2 всички услуги, операции, системи и дейности по обработване на данни, при които организацията трябва да изпълнява правни или договорни изисквания;

2.1.3 всички местоположения и устройства, използвани за обработване на служебна информация, независимо дали са в офис, при дистанционна работа или хоствани в облачна среда.

2.2 Политиката обхваща:

2.2.1 законодателството за защита на данните, като GDPR на ЕС;

2.2.2 регулации в областта на киберсигурността, като NIS2 на ЕС;

2.2.3 специфични за сектора задължения, когато е приложимо;

2.2.4 клиентски договори, споразумения за неразкриване на информация (NDA) и клаузи за одит;

2.2.5 доброволни сертификации (напр. ISO 27001) и вътрешни политики, които трябва да се прилагат за целите на съответствието.

3. Цели

3.1 Установяване на отчетност: да се възложи ясна отговорност за наблюдение, актуализиране и прилагане на правни, регулаторни и договорни задължения.

3.2 Защита на дружеството: да се сведе до минимум рискът от правни нарушения, глоби, инциденти със сигурността на данните и репутационни щети.

3.3 Готовност за одит: да се поддържат проверими записи, които показват как организацията изпълнява задълженията си по съответствие.

3.4 Подкрепа за интегриране на политиките: да се гарантира, че правните и регулаторните задължения се прилагат последователно във всички политики и процеси.

3.5 Прозрачно управление на изключенията: да се гарантира, че всички изключения по съответствие са документирани, обосновани и одобрени с цел ограничаване на отговорността.

4. Роли и отговорности

4.1 Управител

4.1.1 Носи цялостната отговорност за правното и регулаторното съответствие на организацията.

4.1.2 Поддържа Регистър на съответствието и осигурява неговата актуалност.

4.1.3 Преглежда клиентските договори и гарантира, че специфичните задължения се проследяват и изпълняват.

4.1.4 Одобрява изключения от задълженията по съответствие само когато са правно обосновани и са въведени компенсиращи контроли.

4.2 Външни консултанти (напр. правни, ИТ или по съответствие)

4.2.1 Подпомагат Управителя при идентифициране на приложимите закони, сертификации и задължения (напр. GDPR, NIS2, ISO 27001).

4.2.2 Предоставят насоки за тълкуването на нови регулации или промени в действащото законодателство.

4.2.3 Могат да подпомагат актуализацията на политики, одити или реакцията при нарушения, когато е налице правна експозиция.

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

9. Преглед и актуализация на изискванията

9.1 Планиран годишен преглед

9.1.1 Тази политика трябва да се преглежда на всеки 12 месеца от Управителя.

9.1.2 Прегледът трябва да потвърди:

9.1.2.1 приложимостта към текущия правен и договорен контекст;

9.1.2.2 правилното отразяване на клиентските споразумения и задълженията по услугите;

9.1.2.3 съгласуваността с Регистъра на съответствието и другите политики.

9.2 Актуализации, обусловени от събития

9.2.1 Незабавен преглед се изисква, ако:

9.2.1.1 стане приложим нов закон или регулация (напр. ново правило за защита на данните);

9.2.1.2 клиент добави сложни условия по съответствие в своето споразумение;

9.2.1.3 възникне нарушение или инцидент, свързан с несъответствие;

9.2.1.4 дружеството навлезе в регулиран пазар или сектор.

9.3 Одобрение на актуализациите и управление на версиите

9.3.1 Всички актуализации трябва да бъдат документирани, версионирани и одобрени от Управителя.

9.3.2 Историческите версии трябва да се съхраняват за целите на одит и правна защита.

9.4 Комуникиране на промените

9.4.1 Служителите и външните изпълнители трябва да бъдат информирани за промените в политиката в рамките на 5 работни дни след одобрението.

9.4.2 Всички засегнати доставчици също трябва да потвърдят актуализираните условия, преди да продължат предоставянето на услуги.

10. Свързани политики и връзки

10.1 Тази политика се подпомага и прилага чрез следните SME политики:

10.1.1 P3S – Политика за допустимо използване (AUP): предотвратява поведения, които могат да нарушат правни или договорни условия (напр. неразрешено споделяне на файлове).

10.1.2 P8S – Политика за информираност и обучение по информационна сигурност: обучава персонала относно задълженията по съответствие и как да избягва нарушения.

10.1.3 P14S – Политика за съхранение на данни и унищожаване: осигурява законосъобразни практики за обработване на данни през целия им жизнен цикъл.

10.1.4 P17S – Политика за защита на данните и поверителност: изпълнява изискванията на GDPR и изискванията на клиентите за обработване на данни.

10.1.5 P30S – Политика за реагиране при инциденти: определя начина за реагиране при инциденти със сигурността на данните или случаи на несъответствие, включително срокове за уведомяване.

10.1.6 P36S – Политика за социални медии и външни комуникации: гарантира, че публичните комуникации не нарушават правни или регулаторни задължения.

10.2 Всяка свързана политика прилага част от рамката за правно съответствие и трябва да се прилага съгласувано с останалите.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 6.1 – Действия за адресиране на рискове и възможности: включва рискове, свързани със съответствието.

11.1.2 Клауза 8.1 – Оперативно планиране и контрол: изисква изпълнение на процеси, които отговарят на правни и договорни изисквания.

11.2 ISO/IEC 27002

11.2.1 Контрол 5.36 – Насочва организацията при поддържане на записи на задълженията и осигуряване на адекватен отговор на правни и регулаторни изисквания.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Политика и процедури: изисква официални политики по съответствие.

11.3.2 PM-1 – План на програмата по информационна сигурност: изисква интегриране на правното съответствие в планирането на сигурността.

11.3.3 CA-1 – Оценяване, оторизация и мониторинг.

11.3.4 AU-1 – Политика за одит: изисква поддържане на доказателства за съответствие.

11.4 GDPR на ЕС

11.4.1 Член 5 – Принципи на обработването на данни, включително принципа на отчетност.

11.4.2 Член 6 – Правно основание за обработване.

11.4.3 Член 32 – Сигурност на обработването.

11.4.4 Член 33 – Уведомяване за нарушение в рамките на 72 часа.

11.5 Директива NIS2 на ЕС

11.5.1 Член 21(2)(a) и (f) – Вътрешни политики за контрол на риска и регулаторен надзор.

11.5.2 Член 23 – Прилагане и санкции при неизпълнение на изискванията за съответствие.

11.6 Регламент DORA на ЕС

11.6.1 Член 5(2) – Надзор върху управлението на риска в областта на ИКТ.

11.6.2 Член 9(1) – Вътрешно управление на съответствието.

11.6.3 Член 17 – Договорни отношения с доставчици на ИКТ услуги.

11.7 COBIT 2019

11.7.1 APO12 – Управляван риск: гарантира, че рисковете по съответствие се проследяват и адресират.

11.7.2 APO13 – Управлявана сигурност: обхваща прилагането на регулаторното и договорното съответствие, базирано на риска.

11.7.3 DSS01 – Управлявани операции: изисква оперативна готовност за изпълнение на правни задължения.