

ПОЛИТИКА 08 · KRB-POL-08



Политика конфиденциальности и информационной безопасности



НАИМЕНОВАНИЕ ДОКУМЕНТА Политика конфиденциальности и информационной безопасности	№ ДОКУМЕНТА KRB-POL-08	ДАТА ПУБЛИКАЦИИ 03.03.2025
№ / ДАТА РЕДАКЦИИ 1 / 11.08.2026	ПОДГОТОВИЛ Юридический отдел и отдел комплаенса	УТВЕРДИЛ Совет директоров

8.1 © Цель

Целью настоящей Политики является определение принципов, правил и обязанностей по защите конфиденциальной информации, коммерческой тайны, объектов интеллектуальной собственности и персональных данных, принадлежащих Karub Enerji или доверенных ей третьими лицами, а также обеспечение конфиденциальности, целостности и доступности информации.

Для Karub Enerji как наукоёмкой технологической компании информация — такая как рецептуры производства ячеек и модулей, параметры процессов, данные испытаний, файлы проектирования и сведения о клиентах — относится к числу наиболее ценных активов.

8.2 👤 Область применения

Настоящая Политика охватывает всю информацию, принадлежащую Компании или находящуюся под её контролем, независимо от носителя (бумажного, электронного, устного или визуального), а также всех работников, руководителей, стажёров, консультантов, поставщиков и деловых партнёров, имеющих доступ к этой информации. Обязательства сохраняют силу и после прекращения деловых отношений.

8.3 📄 Правовая основа

- Закон № 6698 о защите персональных данных и подзаконные акты к нему, а также решения Совета по защите персональных данных
- Стандартные договоры, обязательные корпоративные правила и механизмы явного согласия для трансграничной передачи в соответствии со ст. 9 Закона № 6698
- Закон № 5651 о регулировании публикаций в интернете
- Ст. 396 (запрет конкуренции) и положения о недобросовестной конкуренции (ст. 54 и след.) Торгового кодекса Турции № 6102
- Ст. 396 (обязанность лояльности работника) и ст. 444–447 (запрет конкуренции) Обязательственного кодекса Турции № 6098
- Ст. 135–140 (преступления в отношении персональных данных) и ст. 239 (разглашение сведений, составляющих коммерческую тайну) Уголовного кодекса Турции № 5237

- Закон о промышленной собственности № 6769 и Закон об интеллектуальных и художественных произведениях № 5846
- Общий регламент ЕС по защите данных (GDPR) — в применимой мере
- Стандарт ISO/IEC 27001 «Системы менеджмента информационной безопасности»

8.4 Определение и классификация конфиденциальной информации

Конфиденциальная информация — это любая информация, не являющаяся общедоступной, раскрытие которой может причинить ущерб Компании, её работникам, клиентам или деловым партнёрам. К ней, в частности, относятся: производственные рецептуры и параметры процессов, технические чертежи и проекты, результаты проектов НИОКР и испытаний, изобретения, по которым ещё не подана патентная заявка, данные о себестоимости и ценообразовании, информация о предложениях и тендерах, списки клиентов и поставщиков, условия договоров, финансовые данные и бизнес-планы, сведения о персонале и заработной плате, информация о безопасности информационных систем.

Информация классифицируется по четырём уровням: «Открытая», «Для внутреннего использования», «Конфиденциальная» и «Строго конфиденциальная». Для каждого класса отдельно определяются правила доступа, хранения, передачи, копирования и уничтожения, и документы соответствующим образом маркируются.

8.5 Основные обязательства по конфиденциальности

- ◆ Конфиденциальная информация используется только в объёме, необходимом для работы, и в рамках принципа «необходимо знать» (need-to-know).
- ◆ Конфиденциальная информация не может передаваться неуполномоченным лицам — включая других работников Компании.
- ◆ Обмен информацией с третьими лицами должен основываться на заранее подписанном письменном соглашении о неразглашении (NDA).
- ◆ Конфиденциальная информация не может копироваться на личные устройства, в личные учётные записи электронной почты, неутверждённые облачные сервисы или съёмные носители.
- ◆ Конфиденциальная информация не может распространяться в социальных сетях, на конференциях, в пресс-релизах или в общедоступных инструментах на основе искусственного интеллекта.
- ◆ При прекращении деловых отношений вся конфиденциальная информация и все содержащие её носители возвращаются Компании; хранение копий не допускается.
- ◆ Обязательство по конфиденциальности сохраняется бессрочно после прекращения трудового договора.
- ◆ Запрещено получение и использование информации о конкурентах от третьих лиц незаконными способами.

8.6 Защита персональных данных

Компания в качестве оператора данных соблюдает общие принципы, установленные ст. 4 KVKK, в отношении обрабатываемых ею персональных данных: законность и добросовестность; точность и при необходимости актуальность; обработка в конкретных, явных и законных целях; связанность с целью, ограниченность и соразмерность; хранение в течение срока, предусмотренного законодательством или необходимого для целей обработки.

- ◆ Персональные данные обрабатываются только при наличии одного из условий обработки, перечисленных в ст. 5 и 6 KVKK.
- ◆ Субъекты данных информируются в соответствии со ст. 10 KVKK до начала обработки; при необходимости получается явное согласие, и сообщается о возможности его отзыва.

- ◆ Составляется и поддерживается в актуальном состоянии Реестр обработки персональных данных; обязательство по регистрации в VERBİS выполняется в той мере, в какой Компания подпадает под его действие.
- ◆ Сроки хранения определяются в соответствии с Политикой хранения и уничтожения персональных данных; по истечении срока данные удаляются, уничтожаются или анонимизируются.
- ◆ С контрагентами, оказывающими услуги в качестве обработчиков данных, заключаются соглашения об обработке данных, соответствующие KVKK.
- ◆ Трансграничная передача осуществляется в рамках ст. 9 KVKK на основании решения об адекватности, надлежащих гарантий (стандартные договоры, обязательные корпоративные правила) или исключений, с соблюдением обязательств по уведомлению Уполномоченного органа.
- ◆ Запросы субъектов данных рассматриваются не позднее тридцати дней в соответствии с Коммюнике о порядке и принципах обращения к оператору данных.
- ◆ Мероприятия по мониторингу работников (видеонаблюдение, журналирование, отслеживание транспортных средств, контроль электронной почты) проводятся только в законных целях, соразмерно и с предварительным уведомлением работников.
- ◆ Использование файлов cookie на корпоративном веб-сайте управляется прозрачно посредством отдельной Политики cookie и инструмента управления cookie; для необязательных cookie получается явное согласие.

8.7



Защита прав интеллектуальной и промышленной собственности

Права на изобретения, проекты, программное обеспечение и произведения, созданные работниками в рамках исполнения трудовых обязанностей, принадлежат Компании в соответствии с законодательством и условиями договоров. Процедуры уведомления и вознаграждения за служебные изобретения осуществляются в соответствии с положениями Закона о промышленной собственности. Технические решения, по которым планируется подача патентной заявки, ни при каких обстоятельствах не раскрываются до даты подачи заявки; в отношении информации, которую предпочтительно защищать как коммерческую тайну, применяются ограничения доступа. Уважаются права интеллектуальной собственности третьих лиц; использование нелицензионного программного обеспечения запрещено.

8.8



Меры информационной безопасности

- ◆ **Технические меры:** межсетевой экран и сегментация сети, защита конечных устройств и обнаружение вредоносного ПО, шифрование дисков и каналов передачи, многофакторная аутентификация, управление полномочиями и ролевым доступом, журналирование и мониторинг, управление обновлениями и уязвимостями, регулярное резервное копирование и тестирование восстановления из резервных копий.
- ◆ **Организационные меры:** обучение по повышению осведомлённости в области информационной безопасности, имитации фишинговых атак, практика чистого стола и чистого экрана, обязательства о конфиденциальности, процессы предоставления и отзыва полномочий при приёме и увольнении, оценка безопасности поставщиков.
- ◆ **Физические меры:** контроль доступа по картам в производственные зоны, серверные помещения и лаборатории НИОКР, регистрация и сопровождение посетителей, видеонаблюдение в критических зонах, использование запираемых шкафов и уничтожителей документов для бумажных носителей.
- ◆ Несанкционированная фото- и видеосъёмка в производственных и лабораторных зонах запрещена.
- ◆ Разрабатываются и регулярно тестируются планы обеспечения непрерывности деятельности и аварийного восстановления.

8.9

Управление инцидентами

О любом фактическом или предполагаемом инциденте информационной безопасности и утечке данных незамедлительно сообщается в Отдел информационных технологий и Юридический отдел/отдел комплаенса. Инциденты управляются в соответствии с процедурой реагирования, включающей этапы обнаружения, локализации, анализа коренных причин, устранения и отчётности. В случае утечки персональных данных Совет по защите персональных данных уведомляется в кратчайшие сроки и в любом случае в течение семидесяти двух часов; затронутые субъекты данных информируются в разумно короткий срок. Ведётся учёт инцидентов, и принимаются меры по предотвращению повторения аналогичных событий.

8.10

Санкции, мониторинг и вступление в силу

Нарушение настоящей Политики может повлечь дисциплинарные взыскания вплоть до расторжения трудового договора по уважительной причине, ответственность за возмещение ущерба, а в отношении деяний, образующих состав преступления, — уголовную ответственность. При нарушениях со стороны третьих лиц применяются договорные санкции, и отношения могут быть прекращены.

Эффективность Политики отслеживается по количеству инцидентов и времени реагирования, доле прошедших обучение по повышению осведомлённости, показателям успешности имитаций фишинга, количеству запросов субъектов данных и сроку ответа, а также результатам аудитов. Политика пересматривается не реже одного раза в год или незамедлительно при изменении законодательства и вступает в силу после утверждения Советом директоров.

подготовил

**Юридический отдел и отдел
комплаенса**

.....
Ф.И.О. / Подпись / Дата

УТВЕРДИЛ

Совет директоров

.....
Ф.И.О. / Подпись / Дата