ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ, ХРАНЕНИЯ И УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ЦЕЛЬ

Цель настоящей Политики хранения и уничтожения персональных данных («в дальнейшем «Политика»);

Компания «YAZICI TURİZM MARMARIS İŞLETMELERİ A.Ş.» («Отель Grand Yazıcı Club Turban» или «Ответственный за данные») несет ответственность за определение периодов обработки персональных данных, а также определение критериев и методов удаления, уничтожения или анонимизации персональных данных, срок обработки которых истек и/или цель обработки которых прекратилась, назначает людей и распределяет обязанности персонала, которые будут принимать участие в данных процессах.

Настоящая политика также включает технические и административные меры, принятые для обеспечения безопасности данных, как указано в статье 6 «Положения об удалении, уничтожении или анонимизации персональных данных», вступившего в силу 28 октября 2017 года. В этом контексте также были приняты во внимание положения из «Положения о реестре ответственных за данные» от 30 декабря 2017 года и «Руководства по удалению, уничтожению и анонимизации персональных данных».

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

О данной Политике: в соответствии со статьей 7 Закона «О защите персональных данных № 6698 («KVKK»)», отель Grand Yazıcı Club Turban, как «ответственный за данные», обрабатывает электронные данные и охватывает удаление, уничтожение или анонимизацию всех персональных данных, которые находятся в в бумажной форме и/или сроки обработки которых истекли.

3.ОПРЕДЕЛЕНИЯ

Среди конкретных определений, включенных в этот документ присутствует:

Прямое согласие: Согласие относительно конкретного предмета, основанное на информации и выраженное по свободной воле,

Отель Grand Yazıcı Club Turban

/ «ответственный за данные: Компания «Yazıcı Turizm Marmaris İşletmeleri A.Ş.»

Анонимизация : Компания обязана обеспечить, чтобы персональные данные не могли быть каким-либо образом связаны с идентифицированным или идентифицируемым физическим лицом, даже если они сопоставляются с другими данными.

Удаление : каким-либо образом сделать персональные данные недоступными и непригодными для использования соответствующими пользователями.

Аннулирование : сделать персональные данные недоступными, безвозвратными и непригодными для любого использования каким-либо образом.

Уничтожение : Удаление, уничтожение или анонимизация персональных данных

Законодательная база: «Закон о защите персональных данных № 6698».

Персональные данные: Любая информация об идентифицированном или идентифицируемом физическом лице.

Физическое лицо : Реальное лицо, чьи персональные данные обрабатываются.

Обработка персональных данных: Любая операция, выполняемая с данными, такая как классификация или предотвращение их использования, получение, запись, хранение, сохранение, изменение, переупорядочение, раскрытие, передача, присвоение, предоставление, классификация или использование персональных данных полностью или частично автоматическими или неавтоматическими способами при условии, что они являются частью какой-либо системы регистрации данных.

Совет (орган) : Совет по защите персональных данных.

Инвентаризация обработки персональных данных: Действия по обработке персональных данных, осуществляемые ответственным за данные лицом в зависимости от его бизнес-процессов; инвентаризация, созданная путем ее связывания с целями обработки персональных данных, категорией данных, переданной группой получателей и группой субъектов данных, а также с указанием максимального периода, необходимого для целей обработки персональных данных, подлежащих передаче в зарубежные страны, и мер принятые в отношении безопасности данных.

Особые персональные данные : Данные о расе, этническом происхождении, политических взглядах, философских убеждениях, религии, сектах или других убеждениях, внешнем виде и одежде, членстве в ассоциациях, фондах или союзах, здоровье, сексуальной жизни, судимости и мерах безопасности, а также биометрические и генетические данные.

Третья сторона : Третье физическое или юридическое лицо, кроме компании, которой передаются персональные данные внутри страны или за рубежом.

Лицо, ответственное за контроль данных

Контактное лицо : относится к реальному лицу, назначенному ответственным за данные, которое осуществляет административное отслеживание процессов, установленных в рамках Закона.

4. РАЗЪЯСНЕНИЕ ОТНОСИТЕЛЬНО ЮРИДИЧЕСКИХ, ТЕХНИЧЕСКИХ ИЛИ ДРУГИХ ПРИЧИН, ТРЕБУЮЩИХ ХРАНЕНИЯ И УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ.

Отель Grand Yazıcı Club Turban обрабатывает персональные данные сотрудников, кандидатов на работу, поставщиков / субподрядчиков, посетителей, онлайн-посетителей и клиентов с целью выполнения бизнес-процессов, выполняемых его подразделениями, в соответствии с должностными инструкциями и действиями, связанными с этими процессами. Компания хранит эти персональные данные в течение сроков, предусмотренных законодательством или определяемых соответствующим ведомством в рамках цели обработки персональных данных. Весь этот поток включен в Реестр обработки персональных данных. По истечении соответствующих сроков хранения персональные данные, цель обработки которых устранена, уничтожаются способами удаления, уничтожения или анонимизации, указанными в настоящей Политике.

5. ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРЫ, ПРИНИМАЕМЫЕ ДЛЯ БЕЗОПАСНОГО ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПРЕДОТВРАЩЕНИЯ ИХ НЕЗАКОННОЙ ОБРАБОТКИ И ДОСТУПА К ИХ.

В этом разделе описаны технические и административные меры, принятые отелем Grand Yazıcı Turban. Отель Grand Yazıcı Club Turban хранит персональные данные в надежном месте на бумажных и электронных носителях в соответствии со своим назначением и в течение указанных периодов. Только люди, уполномоченные руководством отеля Grand Yazıcı Club Turban, могут получить доступ к персональным данным, и это разрешение классифицируется в зависимости от обработки персональных данных.

6. ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРЫ, ПРИНИМАЕМЫЕ ДЛЯ ЗАКОННОГО УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ.

Персональные данные, хранящиеся в базе данных отеля Grand Yazıcı Club Turban, в случае устранения цели обработки, без ущерба для правовых норм, законного срока хранения, предусмотренного применимыми правовыми нормами, в случае истечения периода, необходимого для цели обработки, или по истечении срока по запросу соответствующего лица и принимая во внимание конфиденциальность данных
- уничтожаются путем удаления, уничтожения или анонимизации.

Сроки хранения всех данных, включенных в Реестр обработки персональных данных, определяются ответственным за данные, с учетом соответствующих законов и правовых норм. Отдел кадров несет ответственность за сроки хранения и уничтожение

персональных данных. Отдел кадров обеспечивает удаление персональных данных таким образом, чтобы персональные данные могли обрабатываться только соответствующими пользователями, а данные не могли обрабатываться и быть доступными для всех других несвязанных между собой отделов. Способы маскировки применяются в объеме, необходимом для персональных данных на электронных носителях. Для персональных данных на бумажном носителе процесс удаления осуществляется путем сокрытия персональных данных, подлежащих удалению.
Для уничтожения данных используются один или несколько из следующих методов:

6.1. Удаление персональных данных.

Удаление персональных данных — это процесс, при котором персональные данные становятся недоступными и непригодными для использования соответствующими пользователями каким-либо образом. Ответственный за данные обязан принять все необходимые технические и административные меры для обеспечения того, чтобы удаленные персональные данные были недоступны и непригодны для использования соответствующими пользователями.

6.1.1. Процесс удаления персональных данных

Процедура удаления персональных данных следующая:

• Определение персональных данных, которые будут подлежать удалению.

• Идентификация соответствующих пользователей для каждых персональных данных с использованием матрицы авторизации и контроля доступа или аналогичной системы.

• Определение полномочий и методов соответствующих пользователей, таких как доступ, извлечение и повторное использование.

• Закрытие и устранение доступа, получения и повторного использования разрешений и методов в рамках персональных данных для соответствующих пользователей.

6.1.2.Методы удаления персональных данных.

a) Тип приложения «Облачные решения как услуга»: в облачной системе данные необходимо удалить, подав команду удаления. При выполнении указанной операции следует учитывать, что соответствующий пользователь не имеет полномочий на восстановление удаленных данных в облачной системе.

b. Персональные данные на бумажном носителе

Персональные данные на бумажном носителе должны быть удалены методом затемнения, зачеркивания. Процесс затемнения/зачеркивания данных осуществляется

путем удаления личных данных из соответствующего документа, когда это возможно, а в случаях, когда это невозможно, то необходимо сделать их визуально невидимыми или нечитаемыми для соответствующих пользователей с использованием нестираемых чернил с необратимым эфектом с помощью технологических решений.

c. Файлы Office на центральном сервере

Файл необходимо удалить командой удаления в операционной системе или удалить права доступа соответствующего пользователя к файлу или каталогу, в котором находится файл. При выполнении указанной операции следует учитывать, что соответствующий пользователь не является одновременно системным администратором.

d. Персональные данные на портативных носителях

Персональные данные на флэш-носителях следует хранить в зашифрованном виде и удалять с помощью программного обеспечения, подходящего для этих носителей.

e. Базы данных

Соответствующие строки, содержащие персональные данные, необходимо удалить командами базы данных (DELETE и т.п.). При выполнении указанной операции следует учитывать, что соответствующий пользователь не является одновременно администратором базы данных.

Персональные данные на бумажных и электронных носителях, цель обработки которых полностью исключена, уничтожаются в соответствии с «Руководством по удалению, уничтожению или обезличиванию персональных данных», опубликованным Органом по защите персональных данных, либо обезличиваются способами, предусмотренными настоящим Руководством. Все операции по удалению, уничтожению или анонимизации, выполняемые отделом кадров, протоколируются и фиксируются в электронном виде с отметкой времени. По персональным данным на бумажных носителях отчет о совершении данных операций составляется и хранится в отделе кадров. Записи об удалении, уничтожении или обезличивании персональных данных на электронных и бумажных носителях хранятся в течение трех лет. Отель Grand Yazıcı Club Turban использует метод «удаления», чтобы гарантировать, что только соответствующие отделы будут иметь доступ к персональным данным в течение периода их хранения. Если срок хранения истекает и нет иной цели, требующей хранения персональных данных, используется метод анонимизации.

6.2. Уничтожение Персональных данных.

Уничтожение персональных данных — это процесс, делающий персональные данные недоступными, безвозвратными и непригодными для использования кем-либо. Отель Grand Yazıcı Club Turban обязан принять все необходимые технические и административные меры относительно уничтожения персональных данных.

6.2.1.Методы уничтожения персональных данных

Чтобы уничтожить персональные данные, все копии данных должны быть идентифицированы и уничтожены одна за другой, используя один или несколько из следующих методов, в зависимости от типа систем, в которых расположены данные:

a) Локальные системы

Для уничтожения данных в рассматриваемых системах можно использовать один или несколько из следующих методов.

i) Физическое разрушение: это процесс физического разрушения оптических и магнитных носителей, такой как плавление, сжигание или измельчение. Данные становятся недоступными из-за таких процессов, как плавление оптических или магнитных носителей, их сжигание, измельчение или пропускание через металлический измельчитель. Для твердотельных дисков, если перезапись или размагничивание не увенчались успехом, этот носитель также необходимо физически уничтожить.

ii) Перезапись: это процесс предотвращения восстановления старых данных путем записи случайных данных, состоящих из 0 и 1, не менее семи раз на магнитные носители и перезаписываемые оптические носители. Этот процесс осуществляется с помощью специального программного обеспечения.

b) Экологические системы

Ниже перечислены методы утилизации, которые можно использовать в зависимости от типа окружающей среды:

i) Сетевые устройства (коммутатор, маршрутизатор и т. д.): носители данных в этих устройствах являются фиксированными. Продукты часто имеют команду удаления, но не имеют функции уничтожения. Он должен быть уничтожен с использованием одного или нескольких соответствующих методов, указанных в пункте (a).

ii) Носители на основе флэш-памяти: жесткие диски на основе флэш-памяти с интерфейсом ATA (SATA, SSD, PATA и т. д.), SCSI (SCSI Express и т. д.) можно использовать с командой <block стереть>, если она поддерживается или нет. Если поддерживается, используйте метод уничтожения, рекомендованный производителем, или оно должно быть уничтожено с использованием одного или нескольких соответствующих методов, указанных в пункте (a).

iii) Мобильные телефоны (Sim-карта и постоянные области памяти): в фиксированных областях памяти портативных смартфонов есть команда удаления, но большинство из них не имеют команды уничтожения. Он должен быть уничтожен с использованием одного или нескольких соответствующих методов, указанных в пункте (a).

iv) Периферийные устройства, такие как принтеры со съемными носителями записи данных: необходимо убедиться, что все носители записи данных были удалены и уничтожены с использованием одного или нескольких соответствующих методов, указанных в пункте (a), в зависимости от их характеристик.

v) Периферийные устройства, такие как принтеры с фиксированными носителями для записи данных: большинство рассматриваемых систем имеют команду удаления, но не имеют команды уничтожения. Он должен быть уничтожен с использованием одного или нескольких соответствующих методов, указанных в пункте (a).

c) Бумажные носители

Поскольку персональные данные на этих носителях постоянно и физически записываются на носитель, основная среда должна быть уничтожена с помощью измельчителей бумаги или клипсаторов. При выполнении этого процесса необходимо разделить бумажный носитель на небольшие кусочки такого размера, при чтобы их нельзя было собрать обратно, и по возможности перемешать.

Персональные данные, переданные из исходного бумажного формата в электронную среду путем сканирования, должны быть уничтожены с использованием одного или нескольких соответствующих методов, указанных в пункте (a), в зависимости от электронной среды, в которой они находятся.

d) Облачная среда

При хранении и использовании персональных данных в рассматриваемых системах они должны шифроваться криптографическими методами и, по возможности, использоваться отдельные ключи шифрования для персональных данных, особенно для каждого облачного решения, от которого получена услуга. Когда прекращаются отношения со службой облачных вычислений, все копии ключей шифрования, необходимые для использования персональных данных, должны быть уничтожены.

Помимо указанных носителей уничтожение персональных данных в устройствах, вышедших из строя или отправленных на техническое обслуживание, осуществляется следующим образом:

i) Уничтожение содержащихся в нем персональных данных с использованием одного или нескольких соответствующих методов, указанных в пункте (a), перед передачей их третьим учреждениям, таким как производители, продавцы и службы по техническому обслуживанию и ремонту соответствующих устройств.

ii) В случаях, когда уничтожение невозможно или нецелесообразно, следует разобрать и сохранить носитель данных и отправить другие дефектные части третьим организациям, таким как производители, дилеры и сервисные службы.

iii) Должны быть приняты необходимые меры предосторожности, чтобы персонал, приходящий извне для таких целей, как техническое обслуживание и ремонт, не копировал личные данные и не выносил их из учреждения.

6.3. Анонимизация персональных данных

Обезличивание (анонимизация) персональных данных означает невозможность каким-либо образом связать персональные данные с идентифицированным или идентифицируемым физическим лицом, даже если они совпадают с другими данными.

Для того, чтобы персональные данные были анонимизированы: персональные данные должны быть возвращены ответственным за данные или группами получателей и/или сделать невозможным их связь с идентифицированным или идентифицируемым физическим лицом, даже за счет использования соответствующих методов с точки зрения среды записи и соответствующей сферы деятельности, таких как сопоставление данные с другими данными.

Ответственный за данные обязан принять все необходимые технические и административные меры для обезличивания персональных данных. Обезличивание персональных данных осуществляется следующими способами в соответствии с принципами, указанными в политике хранения и уничтожения персональных данных.

7. **ПРОЦЕССЫ УНИЧТОЖЕНИЯ ДАННЫХ**

7.1. ТАБЛИЦА ПЕРИОДА ХРАНЕНИЯ И УТИЛИЗАЦИИ.

Сроки хранения в соответствии с типами данных указаны в Реестре персональных данных. Сроки хранения, указанные в соответствующем базовом законодательстве, но не ограничиваясь указанными, указаны в ПРИЛОЖЕНИИ: Таблица сроков хранения. Однако в случае внесения изменений в соответствующее законодательство, указанное в таблице сроков хранения, новое обновленное законодательство будет принято во внимание.

7.2. Период периодического разрушения

Отель Grand Yazıcı Club Turban удаляет/уничтожает/обезличивает персональные данные, срок хранения которых истек и для которых нет иной цели обработки данных,

требующей хранения персональных данных, в течение 6 (шести) месяцев после истечения срока хранения. За этим следит отдел кадров в рамках процесса периодического уничтожения.

7.3. Уничтожение персональных данных по запросу Соответствующего лица. Когда соответствующее лицо запрашивает удаление или уничтожение своих личных данных, обратившись в отель Grand Yazıcı Club Turban.

а) если устранены все условия обработки персональных данных, то отель Grand Yazıcı Club Turban удаляет, уничтожает или анонимизирует персональные данные, подлежащие запросу. Grand Yazıcı Club Turban завершает обработку запросов соответствующих лиц на удаление или уничтожение не позднее «тридцати дней».

б) если все условия обработки персональных данных устранены и персональные данные, являющиеся предметом запроса, переданы третьим лицам - отель Grand Yazıcı Club Turban уведомляет третью сторону об этой ситуации и просит удалить или уничтожить соответствующие персональные данные.

в) Если все условия обработки персональных данных не устранены, этот запрос может быть отклонен отелем Grand Yazıcı Club Turban с объяснением причины в соответствии с третьим пунктом статьи 13 Закона о защите персональных данных, и ответ на отказ будет быть отправлено соответствующему лицу в письменной или электронной форме не позднее, чем в течение **«тридцати дней»,** о чем сообщается в электронной среде.

ПОЛИТИКА ДОСТАТОЧНЫХ МЕР ПРЕДОСТОРОЖНОСТИ ПРИ ОБРАБОТКЕ СПЕЦИАЛЬНЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ВВЕДЕНИЕ

Компания «YAZICI TURİZM MARMARIS İŞLETLMELERI A.Ş.» (Отель «Grand Yazıcı Club Turban» или «Компания») в рамках соответствующих процессов и мероприятий по обработке персональных данных (Закон о защите персональных данных № 6698 («KBKK»), по которому особые категории персональных данных обрабатываются в соответствии со статьей 6. Эти особые категории персональных данных, обрабатываемые Компанией включает в себя опись обработки персональных данных с учетом целей и условий обработки данных. KBKK ст. 6 регламентирует условия обработки специальных персональных данных в своих втором и третьем абзацах. Четвертый абзац гласит, что при обработке специальных персональных данных в дополнение ко всем техническим и административным мерам, которые необходимо принять в соответствии со статьей 12, необходимо принять адекватные меры, которые определяются Советом KBK («Совет»). Данное решение Правления, упомянутое в пункте 6/f.4, было опубликовано в Официальном бюллетене от 7 марта 2018 года.

Цель и сфера действия Политики

Настоящая Политика в соответствии с решением Правления отеля Grand Yazıcı Club Turban объясняет адекватные меры предосторожности, которые должны быть приняты в отношении особых персональных данных, которые обрабатываются, связывая их с безопасностью персональных данных, опубликованной Управлением по защите персональных данных («Учреждение»).

Настоящая Политика распространяется на электронные и бумажные носители, в которых обрабатываются конфиденциальные персональные данные.

В рамках Политики.

1. Действия, предпринимаемые в отношении сотрудников и клиентов при обработке специальных персональных данных

a. Обучение: Сотрудники должны проходить регулярное обучение по вопросам безопасности специальных персональных данных в соответствии с KVKK и соответствующим подзаконным актам, а также решениями и руководствами Совета директоров.

b. Соглашение или обязательство о конфиденциальности: Заключение соглашения или обязательства о конфиденциальности, в частности, в области специальных персональных данных, должно быть в дополнении к трудовому договору, заключенному с сотрудниками, имеющими доступ к конфиденциальным персональным данным. Обязательство о бессрочной конфиденциальности в отношении персональных данных должно быть закреплено как в трудовом договоре, соглашении о конфиденциальности, так и в письме-обязательстве. В случае нарушения соглашений о конфиденциальности должен быть предусмотрен процесс сообщения о нарушениях и процедура, подробно описывающая этот процесс, а в случае нарушения соглашения о конфиденциальности должны быть предприняты необходимые действия. Для защиты информационных активов отель Grand Yazıcı Club Turban должен подписывать соглашение о конфиденциальности со всеми поставщиками, третьими лицами, сотрудниками, работающими по контракту, и субподрядчиками поставщиков, которым предоставляется доступ к критически важным информационным активам.

c. Разрешения и средства контроля доступа. Необходимо четко определить объем и продолжительность полномочий сотрудников, которым разрешен доступ к конфиденциальным персональным данным. Кроме того, эти полномочия необходимо периодически проверять. Для этого необходимо создать матрицу авторизации и контроля доступа в рамках Руководства по безопасности данных, опубликованного Управлением KVK. Права доступа к конфиденциальным персональным данным сотрудников, увольняющихся с работы или чьи обязанности меняются, должны быть немедленно аннулированы, а записанное на них электронное оборудование должно быть возвращено. При определении ролей и ответственности в организационной структуре следует по возможности учитывать принципы разделения обязанностей и наименьших прав доступа. При такой структуре одному и тому же человеку не следует назначать

несовместимые обязанности. Если обязанности сотрудников отеля Grand Yazıcı Club Turban меняются, необходимо внести изменения в их старые полномочия, прежде чем назначать новые/дополнительные полномочия в соответствии с новыми обязанностями. Grand Yazıcı Club Turban должен обеспечить регулярное увольнение сторонних сотрудников и определение соответствующих обязанностей в указанном отеле. Прежде чем проводить собеседование с сторонними сотрудниками, уволенными с работы или проекта, все права доступа уволившегося с работы сотрудника должны быть удалены, а затем все активы, принадлежащие отелю Grand Yazıcı Club Turban, должны быть возвращены. В случае увольнения или по истечении срока их контракта, сотрудники третьей стороны должны передать свои активы уполномоченному персоналу отеля Grand Yazıcı Club Turban. Любой доступ к информационным системам и сервисам, содержащим конфиденциальные персональные данные, должен осуществляться посредством процедуры регистрации пользователя, обеспечивающей подтверждение права доступа до предоставления доступа. Должен соблюдаться процесс удаления доступа, который также обеспечит автоматическое или своевременное уведомление об удалении доступа к информационным системам и услугам. Доступ третьих лиц к информационным системам, содержащим конфиденциальные персональные данные, должен быть обеспечен после детального анализа данного требования и оценки связанных с этим рисков.

2. Соответствующие меры предосторожности, которые следует принимать в электронной среде, где обрабатываются, хранятся и доступны специальные персональные данные.

a. Электронные носители, содержащие конфиденциальные персональные данные, должны храниться криптографическими методами.

b. Чтобы обеспечить безопасность ключей, используемых для этой цели, необходимо обеспечить их безопасность, храня их в разных безопасных средах.

c. Все транзакции и записи, сделанные с конфиденциальными личными данными, должны регистрироваться. Необходимо вести и отслеживать журналы действий пользователей, исключений и событий безопасности. Журналы аудита должны включать следующее:

Время начала и окончания

• Системные ошибки или неисправности и принятые меры по их устранению.

• Проверка и правильная обработка файлов данных и выходных данных системы.

• Имя или имя пользователя лица, о котором ведется контрольный журнал.

Действия пользователей с высокими уровнями доступа (привилегированные пользователи, такие как системные администраторы и системные операторы) должны регистрироваться и регулярно проверяться кем-то независимым.

Доступ к приложениям, содержащим конфиденциальные персональные данные, и доступ к сети отеля Grand Yazıcı Club Turban должны контролироваться на предмет любых нарушений безопасности. Для таких ситуаций должны быть созданы соответствующие механизмы. Удаленный доступ должен предоставляться только в ограниченной степени и осуществляться в соответствии с разрешениями, предоставленными через системы.

Аудиторские журналы должны вестись в соответствии с потребностями ведения учета и хранения. Механизмы хранения контрольного журнала и контрольные журналы должны быть защищены от несанкционированного доступа.

d. В случаях, когда доступ к конфиденциальным персональным данным осуществляется через программное обеспечение или среду, в которой эти данные хранятся, необходимо постоянно отслеживать обновления безопасности. Необходимо периодически выполнять необходимые тесты безопасности и планировать необходимые действия, записывая результаты.

e. В случаях, когда требуется удаленный доступ к этим данным, необходимо использовать как минимум двухфакторную систему аутентификации.

f. Важно провести «АНАЛИЗ ВОЗДЕЙСТВИЯ НА ЗАЩИТУ ДАННЫХ» в тех случаях, когда обрабатываемые специальные персональные данные представляют собой биометрические данные, данные о состоянии здоровья и генетические данные.

3. Адекватные меры предосторожности, которые следует принимать в физической среде, где обрабатываются, хранятся и доступны специальные персональные данные.

a. Если средой, в которой хранятся конфиденциальные персональные данные, является архив или центр обработки данных, необходимо принять необходимые меры безопасности для обеспечения технической и физической безопасности этих сред.

b. Средства физической безопасности должны быть разработаны и реализованы для офисов, помещений и объектов в соответствии с содержащимися в них конфиденциальными личными данными.

c. Несанкционированный вход и выход в эти среды должен быть предотвращен.

4. Адекватные меры предосторожности, которые следует принимать при передаче особых персональных данных

a. В тех случаях, когда эти данные необходимо передать по электронной почте, они должны передаваться в зашифрованном виде с использованием корпоративного адреса электронной почты или адреса KEP. Электронные письма, содержащие конфиденциальные персональные данные, следует отправлять, помечая их классами данных, которые в корпорации называются «конфиденциальными» или «конфиденциальными и личными».

b. В тех случаях, когда требуется передача через такие носители, как переносное запоминающее устройство, компакт-диск, DVD, необходимо шифрование криптографическими методами и обеспечение управления ключами и безопасности путем хранения ключей в разных средах.

c. Если передача должна осуществляться между серверами в разных физических средах, передача должна осуществляться путем установки VPN или аналогичных методов.

d. Если требуется передача на бумажном носителе, необходимо принять необходимые меры предосторожности против таких рисков, как кража, потеря или просмотр документа посторонними лицами, а также документ должен быть отправлен в рамках конфиденциальной информации.

** В случае возникновения противоречий между турецкой версией настоящей Политики, в которой она была подготовлена, и любой версией перевода, следует принимать во внимание только текст на турецком языке.