Политика обработки персональных данных

Оглавление

1. Сфера применения. 2

2. Термины и определения. 3

3. Принципы обработки персональных данных. 5

4. Категории субъектов персональных данных, чьи данные подлежат обработке. Состав обрабатываемых персональных данных, цели и сроки обработки. 7

4.1. Работники Компании. 7

4.2. Соискатели на вакантные должности. 8

4.3. Партнеры Компании. 9

4.4. Пользователи официального веб-сайта..... 10

5. Права субъектов персональных данных. 11

6. Правила доступа к персональным данным. Меры по защите персональных данных, используемые в Компании. 15

6.1. Лица, ответственные за обработку персональных данных. 15

6.2. Правила доступа работников Компании к персональным данным. 16

6.3. Правила передачи персональных данных компаниям Группы UTC и третьим лицам, включая трансграничную передачу. 16

6.4. Меры по обеспечению безопасности персональных данных, которые принимаются в Компании..... 17

7. Условия применения простой электронной подписи в системе eService…….18

8. Ответственность за несоблюдение требований к обработке и обеспечению безопасности персональных данных. 21

1. Сфера применения.

1.1. Настоящая Политика обработки персональных данных регламентирует процессы обработки и обеспечения безопасности всех категорий персональных данных в Компании.

1.2. Настоящая Политика распространяется на все действия Компании по обработке персональных данных, включая процессы сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (предоставления доступа), блокирования, удаления, уничтожения персональных данных в информационных системах и на материальных носителях.

1.3. В настоящей Политике Компания информирует Вас о том, какие персональные данные подлежат обработке, для каких целей они используются, каковы права лиц, которым принадлежат обрабатываемые персональные данные, и как обеспечивается безопасность этих данных.

2. Термины и определения.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту Персональных данных).

Деловые контакты – информация об имени физического лица, номере рабочего телефона, о рабочем адресе и адресе корпоративной электронной почты, которая также относится к Персональным данным.

Партнеры (клиенты и контрагенты Компании) – юридические и физические лица, с которыми Компания состоит или состояла в договорных отношениях, включая подрядчиков, поставщиков, агентов, спонсоров, либо лица, с которыми Компания ведет переговоры об оказании услуг / выполнении работ, поставке товаров или сотрудничестве в иной форме.

Пользователи – физические лица – посетители официального веб-сайта Компании https://www.otis.ru.

Компания - любая из компаний ОТИС в России: Общество с ограниченной ответственностью «ОТИС Лифт» (ОГРН 1027802714741), Акционерное общество «МОС ОТИС» (ОГРН 1027700038871), Закрытое акционерное общество «Щербинка ОТИС Лифт» (ОГРН 1025007509086)» Открытое акционерное общество «ТОРУС» (ОГРН 1027700033910), Открытое акционерное общество «Ремонтно-строительное управление по техническому обслуживанию и ремонту лифтов № 3» (ОГРН 1047839014860), а также иные компании, которые в будущем будут входить в состав группы ОТИС Россия, и утвердят данную Политику приказом генерального директора в качестве локального нормативного акта

Инцидент – одно событие или группа событий, которые могут привести к сбоям или нарушению функционирования информационной системы, содержащей Персональные данные, и / или к возникновению угроз безопасности Персональных данных.

Единые Корпоративные Правила – принятые Группой UTC правила трансграничной передачи Персональных данных между компаниями Группы («Binding Corporate Rules»).

Стандартные Контрактные Условия – принятые Группой UTC модельные положения двусторонних договоров о трансграничной передаче Персональных данных («Standard Contract Clauses»).

Оценка рисков безопасности персональных данных – выявление и оценка угроз безопасности Персональных Данных, проводимая в соответствие с п. 6.4.2. настоящей Политики («Privacy Risk Assessment»).

Оценка влияния на безопасность персональных данных – оценка эффективности принимаемых мер по обеспечению безопасности персональных данных, проводимая в соответствие с п. 6.4.3. настоящей Политики («Privacy Impact Assessment»).

3. Принципы обработки персональных данных.

3.1. При обработке персональных данных Компания руководствуется следующими принципами:

(1) Сбор и обработка Персональных данных осуществляется исключительно на законных основаниях;

(2) Обработка Персональных данных осуществляется только в целях, определенных в Главе 4 настоящей Политики, либо в других целях при наличии согласия субъекта Персональных данных на обработку в этих целях, либо для исполнения Компанией установленной законом обязанности, либо в случае угрозы жизни и здоровью субъекта Персональных данных, или при наличии иного установленного законом основания обработки без согласия субъекта Персональных данных;

(3) Обработке подлежат только Персональные данные, которые отвечают целям обработки, в объеме, который минимально необходим для достижения этих целей и не является избыточным;

(4) Не допускается объединение баз данных, содержащих Персональные данные, обработка которых осуществляется в разных целях;

(5) При обработке Персональных данных должна быть обеспечена их точность, достаточность и актуальность по отношению к целям обработки путем удаления / уточнения неполных или неточных данных;

(6) Хранение Персональных данных осуществляется Компанией не дольше, чем этого требуют цели обработки Персональных данных, если срок хранения Персональных данных не установлен применимым законодательством, договором, стороной которого является субъект Персональных данных, или согласием субъекта Персональных данных на обработку. Персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, при истечении установленного срока обработки, при отзыве субъектом Персональных данных его согласия на обработку, если иное не предусмотрено законодательством или договором с субъектом Персональных данных;

(7) Ответственным должностным лицам Компании должны быть предоставлены соответствующие права доступа к Персональным данным, их удаления и уточнения;

(8) Компания должна применять организационные и технические меры по обеспечению безопасности Персональных данных от несанкционированного доступа, повреждения, частичного или полного уничтожения;

(9) Запрещается передача Персональных данных, включая трансграничную передачу, без законных оснований и принятия организационных и технических мер по обеспечению безопасности передаваемых Персональных данных;

(10) Субъекты Персональных данных должны быть уведомлены об обработке их данных, в том числе о составе обрабатываемых данных и о целях обработки;

(11) Направление субъектам Персональных данных маркетинговой рассылки допускается только после получения предварительного согласия субъекта на получение такой рассылки. Рассылка должна предусматривать возможность субъекта Персональных данных отказаться от нее в онлайн режиме;

(12) Принятие решений исключительно на основании автоматизированной обработки Персональных данных, которые порождают юридические последствия в отношении субъекта Персональных данных или затрагивают его права и законные интересы, допускаются только при наличии согласия субъекта Персональных данных в письменной форме;

(13) Обработка специальных категорий Персональных данных допускается только с соблюдением установленных законом требований к такой обработке, включая требование о получении согласия субъекта Персональных данных в письменной форме.

4. Категории субъектов персональных данных, чьи данные подлежат обработке. Состав обрабатываемых персональных данных, цели и сроки обработки.

4.1. Работники Компании.

4.1.1. Персональные Данные работников Компании, с которыми у Компании заключены или были заключены трудовые договоры, обрабатываются в целях исполнения Компанией своих обязательств по трудовым договорам с этими работниками, обеспечения личной безопасности работников, содействия в обучении работников и продвижении по службе, а также с целью соблюдения трудового законодательства Российской Федерации. Перечень Персональных данных работников, которые может обрабатывать Компания, включает следующую информацию:

(1) Фамилия, имя, отчество;

(2) Дата и место рождения;

(3) Данные документа, удостоверяющего личность;

(4) Адрес регистрации и / или фактического проживания;

(5) Номер личного и / или рабочего телефона;

(6) Адрес личной и / или корпоративной электронной почты;

(7) Личная фотография;

(8) Образец личной подписи;

(9) Информация, содержащаяся в трудовой книжке (сведения о стаже работы в Компании и общем трудовом стаже, предыдущих местах работы);

(10) Информация, содержащаяся в документах бухгалтерского и налогового учета, государственного пенсионного страхования и обязательного медицинского страхования работников, включая сведения о заработной плате, премиях (как выплаченных, так и подлежащих выплате), ИНН, СНИЛС, информацию полиса ОМС и листка нетрудоспособности;

(11) Сведения, содержащиеся в документах воинского учета;

(12) Информация о банковском счете работника, на который осуществляется перечисление заработной платы;

(13) Информация об образовании, специальности, квалификации, содержащаяся в документах об образовании, повышении квалификации, прохождении каких-либо курсов, тренингов, тестов;

(14) Сведения, содержащиеся в разрешении на работу (в случае трудоустройства иностранного гражданина);

(15) Сведения о членах семьи работника.

4.1.2. Работники должны быть уведомлены об обработке своих Персональных данных в понятной и доступной форме.

4.1.3. Персональные данные работников обрабатываются в течение всего срока действия трудового договора и по истечении не более чем 5 лет после прекращения трудового договора для нужд бухгалтерского и налогового учета.

4.1.4. Получение Персональных данных работников может осуществляться как путем предоставления их самим работником, так и путем получения данных о работнике от третьих лиц.

4.1.5. Если Персональные данные работника запрашиваются у третьего лица, то работник должен быть заранее уведомлен о целях, предполагаемых источниках и способах получения (передачи) данных, а также о характере получаемых данных. Компания обязана получить предварительное письменное согласие работника на получение Персональных данных таким способом, а также проинформировать его о последствиях отказа давать такое согласие.

4.1.6. Персональные данные работников обрабатываются в информационных системах Компании на территории России и за ее пределами. Компания обеспечивает первичную запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение Персональных данных в информационных системах, находящихся на территории России. Трансграничная передача этих Персональных данных в информационные системы, находящиеся за границей, осуществляется в соответствии с правилами трансграничной передачи данных, установленными Разделом 6.3. настоящей Политики.

4.2. Соискатели на вакантные должности.

4.2.1. Персональные данные соискателей на вакантные должности Компании обрабатываются с целью проведения отбора претендентов на вакантную должность. В случае отказа в приеме на работу со стороны Компании, либо

отказа со стороны соискателя на любом из этапов проведения отбора, Персональные данные соискателя подлежат уничтожению не позднее, чем через 30 дней после такого отказа. Перечень Персональных данных соискателей на вакантные должности, которые может обрабатывать Компания, включает следующую информацию:

(1) Фамилия, имя, отчество;

(2) Дата и место рождения;

(3) Адрес фактического проживания;

(4) Номер телефона;

(5) Адрес личной электронной почты;

(6) Информация об образовании, квалификации, наличии специальных знаний, содержащаяся в документах об образовании, повышении квалификации, прохождении каких-либо курсов, тренингов, тестов.

4.2.2. Соискатели на вакантные должности должны быть уведомлены об обработке своих Персональных данных в понятной и доступной форме перед началом обработки.

4.2.3. Получение Персональных данных соискателей на вакантные должности может осуществляться как путем предоставления их самим соискателем, так и путем получения данных из общедоступных источников (веб-сайты, агрегирующие резюме кандидатов) / от третьих лиц (кадровые агентства) с соблюдением требований настоящей Политики и действующего законодательства.

4.3. Партнеры Компании и представители/сотрудники Партнеров Компании.

4.3.1. Персональные данные Партнеров Компании (физических лиц) и представителей/сотрудников Партнеров Компании обрабатываются с целью заключения договоров с Партнерами Компании, исполнения Компанией своих обязательств по таким договорам, а также с целью поддержания и развития деловых контактов Компании, организации и проведения маркетинговых и иных мероприятий.

4.3.2. Компания обрабатывает Персональные данные Партнеров и их представителей/сотрудников до момента достижения законных целей обработки этих данных, после чего они должны быть уничтожены в течение не более чем 30 дней, если иное не предусмотрено договором с Партнером.

Перечень Персональных данных Партнеров и их представителей/сотрудников, которые может обрабатывать Компания, включает следующую информацию:

(1) Фамилия, имя, отчество;

(2) Год, месяц, дата и место рождения;

(3) Адрес, номер телефона;

(4) Данные документа, удостоверяющего личность;

(5) ИНН;

(6) Информация о банковском счете / счетах Партнера, являющегося физическим лицом, которые используются для перечисления оплаты по договору.

4.3.3. Партнеры и их представители/сотрудники, чьи персональные данные обрабатывает Компания, должны быть уведомлены об обработке их Персональных данных в понятной и доступной форме.

4.4. Пользователи официального веб-сайта.

4.4.1. Компания имеет официальный веб-сайт в сети Интернет: https://www.otis.ru. Компания обрабатывает Персональные данные Пользователей для целей улучшения качества обслуживания, персонализации услуг путем сбора статистики о частоте посещения Пользователями отдельных страниц и разделов веб-сайта.

4.4.2. К Персональным данным Пользователей, которые может обрабатывать Компания, относятся следующие сведения:

(1) IP-адрес и MAC-адрес;

(2) Информация о количестве посещений, посещении конкретных страниц и разделов веб-сайта, получаемая с помощью файлов cookie.

4.4.3. Компания обязана размещать на официальном веб-сайте https://www.otis.ru настоящую Политику обработки персональных данных. Политика должна проходить проверку на актуальность, соответствие действующему законодательству и, в случае необходимости, обновляться каждые 3 года.

5. Права субъектов персональных данных.

5.1. Сбор и обработка Персональных данных осуществляется Компанией с согласия субъекта Персональных данных в следующих случаях:

(1) Получение Персональных данных соискателей на вакантную должность не из общедоступных источников, а от самого соискателя или от третьих лиц (кадровых агентств, иных организаций);

(2) Получение Персональных данных работников от третьих лиц (за исключением общедоступных источников);

(3) Трансграничная передача персональных данных в США и ряд иных стран, характеризуемых российским законодательством как не обеспечивающие адекватной защиты персональных данных;

(4) Рассылка субъектам Персональных данных рекламных и маркетинговых материалов, новостей Компании.

5.2. Субъекты Персональных данных имеют следующие права:

5.2.1. Право на отказ от предоставления согласия на обработку Персональных данных. В этом случае Компания уведомляет субъекта Персональных данных о последствиях такого отказа.

5.2.2. Право на отзыв данного ранее согласия на обработку Персональных данных:

(1) Субъект Персональных данных вправе отозвать письменное согласие на обработку Персональных данных путем направления уведомления по адресам, указанным в п. 5.2.6. или п. 5.2.7. настоящей Политики, с пометкой «отзыв согласия на обработку персональных данных».

Субъект Персональных данных настоящим уведомляется, что отзыв согласия на обработку данных влечет за собой следующие последствия:

(1) Отзыв соискателем на вакантную должность письменного согласия – удаление Персональных данных такого лица из всех информационных систем Компании, невозможность участия этого лица в дальнейшем отборе претендентов на эту должность;

(2) Отзыв согласия, получаемого в рекламных и маркетинговых целях – прекращение рассылки маркетинговых и рекламных материалов, новостей Компании, удаление Персональных данных адресата из списка рассылки Компании.

5.2.3. Компания имеет право продолжить обработку Персональных данных без согласия субъекта в следующих случаях:

(1) Обработка Персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации на Компанию функций, полномочий и обязанностей (например, для исполнения обязанностей, предусмотренных ст. 29 Федерального закона от 6 декабря 2011 г. N 402-ФЗ «О бухгалтерском учете» и хранения данных работников для целей бухгалтерского и налогового учета);

(2) Обработка Персональных данных необходима для заключения договора по инициативе субъекта Персональных данных, либо исполнения договора, стороной которого / выгодоприобретателем / поручителем по которому является субъект Персональных данных (например, договоры, заключаемые с Партнерами, трудовые договоры);

(3) Обработка Персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта Персональных данных;

(4) Обработка Персональных данных необходима для осуществления прав и законных интересов Компании (например, для формирования и развития деловых контактов, организации и проведения маркетинговых мероприятий и пр.);

(5) Осуществляется обработка Персональных данных, доступ неограниченного круга лиц к которым предоставлен самим субъектом Персональных данных либо по его просьбе (общедоступные Персональные данные).

5.2.4. Право на получение субъектом Персональных данных сведений, касающихся обработки этих данных, в том числе такой информации, как:

(1) Подтверждение факта обработки Персональных данных этого лица Компанией;

(2) Правовые основания и цели обработки Персональных данных;

(3) Способы обработки Персональных данных, применяемые Компаний;

(4) Наименование и место нахождения Компании, сведения о лицах (за исключением работников Компании), которые имеют доступ к

Персональным данным на основании договора с Компанией или на основании закона;

(5) Состав обрабатываемых Персональных данных, источники их получения;

(6) Сроки обработки Персональных данных, в том числе сроки их хранения;

(7) Порядок осуществления субъектом Персональных данных прав, предусмотренных настоящей Главой;

(8) Информация об осуществленной и / или предполагаемой трансграничной передаче Персональных данных;

(9) Наименование юридического лица или фамилия, имя, отчество и адрес физического лица, осуществляющего обработку Персональных данных по поручению Компании, если обработка поручена или будет поручена такому лицу;

(10) Иные, предусмотренные законом, сведения.

Для получения указанной выше информации необходимо направить запрос по адресам, указанным в п. 5.2.6. или п. 5.2.7. настоящей Политики с пометкой «запрос о предоставлении доступа к персональным данным». Субъект Персональных данных вправе в этом же порядке требовать от Компании уточнения, обновления его Персональных данных, их блокирования или уничтожения в случае, если Персональные данные являются неполными, устаревшими, неточными, незаконно полученными или являются избыточными по отношению к заявленным Компанией целям обработки.

5.2.5. Право на обжалование действий или бездействий Компании в уполномоченный орган в случае, если субъект Персональных данных полагает, что его права и свободы были нарушены в ходе обработки Персональных данных Компанией.

5.2.6. Все обращения и запросы работников Компании в отношении обработки их Персональных данных могут быть направлены по следующим контактам:

Юридический Департамент	Телефон: 8(495)974-24-40
Privacy Professional	Электронная почта: ymatveychuk@otis.com Телефон: *8(495)974-24-40#4543

5.2.7. Все обращения и запросы иных субъектов Персональных данных в отношении обработки их Персональных данных могут быть направлены по следующим контактам:

Privacy Professional	Электронная почта: ymatveychuk@otis.com Телефон: *8(495)974-24-40#4543

6. Правила доступа к персональным данным. Меры по защите персональных данных, используемые в Компании.

6.1. Лица, ответственные за обработку персональных данных.

6.1.1. Лицом, ответственным за организацию обработки Персональных данных в Компании является Директор по юридическим вопросам Компании. Ответственное лицо действует по указанию Генерального директора Компании и подотчетно ему. Ответственное лицо обязано:

(1) Осуществлять внутренний контроль за соблюдением Компанией и ее работниками действующего законодательства Российской Федерации о Персональных данных, в том числе требований к обеспечению безопасности Персональных данных;

(2) Осуществлять внутренний контроль за соблюдением работниками настоящей Политики, Корпоративной Политики, а также Единых Корпоративных Правил Группы UTC;

(3) Организовывать Оценку рисков безопасности персональных данных и Оценку влияния на безопасность персональных данных;

(4) Ежегодно организовывать обучение работников (тренинги) с целью доведения до сведения работников положений действующего законодательства Российской Федерации о Персональных данных, содержания локальных актов Компании и Группы UTC по вопросам обработки Персональных данных, требований по обеспечению информационной безопасности;

(5) Организовывать прием и обработку обращений и запросов субъектов Персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

6.1.2. Все документы и принятые в Компании типовые шаблоны документов, регулирующие процессы обработки Персональных данных, включая настоящую Политику, другие локальные акты Компании, соглашения о передаче Персональных данных, трудовые договоры и соглашения о конфиденциальности с работниками, уведомления субъектов Персональных данных об обработке данных и формы согласий на обработку данных, ответы на обращения и запросы субъектов Персональных данных, должны предварительно согласовываться с Юридическим департаментом, Директором по юридическим вопросам.

6.2. Правила доступа работников Компании к персональным данным.

6.2.1. Перечень работников Компании, имеющих доступ к различным категориям Персональных данных, устанавливается приказом Генерального директора Компании.

6.2.2. Все работники Компании должны быть ознакомлены с настоящей Политикой и другими локальными актами Компании, регулирующими обработку Персональных данных и обеспечение информационной безопасности. Компания ведет журнал учета работников, ознакомленных с настоящей Политикой.

6.2.3. В отношении обращения с материальными носителями Персональных данных, и Персональными данными, содержащимися в информационных системах, для работников Компании устанавливаются следующие требования:

(1) Соблюдение пропускного режима в помещениях, предназначенных для хранения материальных носителей, содержащих Персональные данные (архивных помещениях);

(2) Ответственное обращение с материальными носителями, содержащими Персональные данные во избежание их утраты или утечки данных (например, потери документов);

(3) Подписание соглашения о конфиденциальности с Компанией, которое распространяется, в том числе на Персональные данные, к которым работник получил доступ в соответствии с настоящей Политикой;

(4) Добросовестное использование технических мер по защите Персональных данных, содержащихся в информационных системах, от несанкционированного доступа, непреднамеренного удаления / уничтожения (например, использование логина и пароля при входе в информационные системы).

6.3. Правила передачи персональных данных компаниям Группы UTC и третьим лицам, включая трансграничную передачу.

6.3.1. При передаче Персональных данных другим компаниям Группы UTC, находящимся за пределами Российской Федерации (трансграничная передача данных), Компания использует Единые Корпоративные Правила.

6.3.2. При трансграничной передаче Персональных данных любым третьим лицам, не входящим в Группу UTC, Компания использует двусторонние

соглашения о передаче Персональных Данных, разработанные на основе Стандартных Контрактных Условий и требований действующего законодательства.

6.3.3. При передаче Персональных данных третьим лицам (за исключением государственных и муниципальных органов власти), в том числе при трансграничной передаче данных, Компания обязывает третьих лиц соблюдать необходимые меры по обеспечению безопасности этих данных, путем внесения соответствующих условий в соглашения о передаче данных этим лицам.

6.3.4. Лица, указанные в п. 6.3.2. - 6.3.3., перед передачей им Персональных данных, должны быть ознакомлены с требованиями настоящей Политики, а, в случае необходимости, также с требованиями других локальных актов Компании, касающихся обеспечения информационной безопасности.

6.4. Меры по обеспечению безопасности персональных данных, которые принимаются в Компании.

6.4.1. Для защиты Персональных данных Компанией предпринимаются следующие правовые, организационные и технические меры:

(1) Принятие локальных актов, определяющих политику Компании в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

(2) Назначение лица, ответственного за обработку персональных данных в Компании;

(3) Определение угроз безопасности Персональных данных при их обработке в информационных системах персональных данных;

(4) Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

(5) Оценка эффективности принимаемых мер по обеспечению безопасности Персональных данных до ввода в эксплуатацию новой / модифицированной информационной системы;

(6) Учет машинных носителей Персональных данных;

(7) Обнаружение фактов несанкционированного доступа к Персональным данным и принятие технических мер по борьбе с несанкционированным доступом;

(8) Восстановление Персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

(9) Установление правил доступа к Персональным данным, обрабатываемым в информационных системах;

(10) Контроль за принимаемыми мерами по обеспечению безопасности Персональных данных и уровня защищенности информационных систем, содержащих Персональные данные.

6.4.2. С целью определения угроз безопасности Персональных данных и разработки стратегии по устранению этих угроз, Компания проводит Оценку рисков безопасности персональных данных, включая оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства о персональных данных. Оценка рисков безопасности персональных данных проводится в отношении всех действий по обработке Персональных данных, указанных в п. 1.4. настоящей Политики.

6.4.3. С целью оценки эффективности принимаемых мер по обеспечению безопасности Персональных данных до ввода в эксплуатацию той или иной информационной системы, Компания проводит Оценку влияния на безопасность персональных данных. Оценка влияния на безопасность персональных данных проводиться в следующих случаях:

(1) Внедрение новой или модифицированной информационной системы, повторяющегося процесса (например, исследования);

(2) Взаимодействие с новым Партнером, либо изменение подходов в работе с прежним Партнером;

(3) Создание, разработка, запуск новой или модифицированной технологии, продукта, услуги, в рамках которых обрабатываются Персональные данные.

Исключение составляют следующие ситуации, при которых Оценка влияния на безопасность персональных данных не проводится:

(1) Взаимодействие с Партнерами, которые не обрабатывают Персональные данные;

(2) Взаимодействие с Партнерами, если оно подразумевает только обмен Деловыми Контактами с ограниченным кругом работников этого Партнера;

(3) Индивидуальные действия работников, такие как, например, отправка письма по электронной почте или телефонный звонок;

(4) Закупка программного обеспечения (если это не новая информационная система / программа, обрабатывающая Персональные данные), продуктов и сырья, если для осуществления закупки достаточно только обмена Деловыми Контактами с ограниченным кругом работников поставщика.

6.4.4. Оценка влияния на безопасность Персональных данных проводится с помощью системы OneTrust.

6.4.5. В случае возникновения Инцидента, работники обязаны придерживаться принятого в Компании Плана противодействия Инцидентам для успешного устранения Инцидента и нивелирования негативных последствий.

7. Условия применения простой электронной подписи в системе eService

7.1 Настоящие положения устанавливают порядок использования простой электронной подписи пользователями системы eService (далее – Система) при их регистрации и работе в Системе посредством веб-сайта https://eservice.otis.com.

7.2 Простой электронной подписью является электронная подпись, которая посредством использования ключа простой электронной подписи (далее - Ключ) подтверждает факт ее формирования определенным пользователем Системы (далее – Пользователь).

7.3 Ключом является сочетание идентификатора (адреса электронной почты Пользователя, указываемого Пользователем при регистрации в Системе) и пароля ключа (последовательности символов, которая формируется с помощью функционала Системы при регистрации Пользователя и впоследствии при смене пароля по инициативе Пользователя).

7.4. Пользователи обязаны обеспечивать конфиденциальность ключа:

(1) хранить в тайне ключ, принимать все возможные меры, предотвращающие нарушение его конфиденциальности;

(2) формировать простую электронную подпись с использованием ключа, полученного в порядке, установленном настоящими Условиями;

(3) в случае нарушения конфиденциальности ключа или его утери незамедлительно заменить ключ.

7.5. Применяемая в Системе простая электронная подпись, сформированная Пользователем, является равнозначной собственноручной подписи данного Пользователя. Электронные документы, формируемые Пользователем в Системе с использованием ключа, признаются равнозначными документам, подписанным собственноручной подписью Пользователя.

7.6 Учитывая указанное в п. 5 выше, согласие на обработку персональных данных, даваемое Пользователем в Системе с использованием ключа, приравнивается к согласию в письменной форме, требуемому Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

7.7. Проверка подлинности простой электронной подписи, которой подписано обращение или электронный документ, осуществляется функционалом Системы.

8. Ответственность за несоблюдение требований к обработке и обеспечению безопасности персональных данных.

8.1. Компания несет гражданско-правовую и административную ответственность за нарушение законодательства о Персональных данных.

8.2. По решению Генерального директора Компании работники привлекаются к дисциплинарной ответственности за:

(1) Нарушение законодательства Российской Федерации о Персональных данных;

(2) Нарушение положений настоящей Политики;

(3) Нарушение положений Корпоративной Политики Группы UTC.