ПОЛИТИКА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Комплаенс Политики - Политика 7.4 - Защита Персональных Данных

Утверждено	Советом менеджеров
Дата создания:	24 августа 2014 г.
Дата последнего изменения:	2 июня 2018 г.
Владелец Политики:	Глава по комплаенс Группы
Контакты:	Глава международной службы комплаенс

В настоящем документе «Компания» или «ERG» означает Eurasian Resources Group S.a.r.l. и включает в себя, если это применимо, все ее прямые и косвенные дочерние компании.

1. Цель политики

1.1. Каждая Компания Группы в ходе осуществления своей коммерческой деятельности собирает, хранит и обрабатывает информацию о физических лицах. В число таких лиц могут входить сотрудники, подрядчики, поставщики, клиенты, члены Совета Менеджеров, директора, акционеры и гости. Компании Группы уважают конфиденциальность Персональных данных вышеупомянутых субъектов и их право знать, как Компании Группы используют их информацию. При этом Компании Группы придерживаются нулевой терпимости по отношению к несоблюдению соответствующего законодательства, включая, но не ограничиваясь, Регламентом (ЕС) 2016/679 Европейского Парламента и Совета от 27 апреля 2016 г. «О защите физических лиц в отношении обработки Персональных данных и о свободном движении таких данных» (Общий регламент ЕС по защите данных).

1.2. Целью данной Политики является:

1.2.1. гарантировать, что каждая Компания Группы осуществляет свою коммерческую деятельность с соблюдением всех применимых законов и нормативных требований в отношении сбора, хранения, обработки и передачи Персональных данных, а также что Персональные данные всегда защищены и обрабатываются в соответствии с требованиями применимого законодательства[1];

1.2.2. определить типы Персональных данных, которые собирают Компании Группы, и цели сбора этих данных;

1.2.3. изложить обязанности каждого сотрудника в отношении сбора и обработки данных согласно положениям применимых нормативно-правовых актов в сфере защиты данных; а также

[1] *Например, в **Европейском союзе** обработка Персональных данных регулируется Общим регламентом по защите данных (General Data Protection Regulation, GDPR) (Постановление (Европейский союз) 2016/679) и другими исполнительными документами. В **Великобритании** это в первую очередь «Закон о защите данных» 2018 года («Закон»), а также другие нормативные акты;*

*В **Швейцарии** – Федеральный закон от 19 июня 1992 «О защите персональных данных»,*
*В **Казахстане** — Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите».*
*В **России** — Федеральный закон Российской Федерации «О персональных данных» от 27 июля 2006 г. № 152-ФЗ с подзаконными актами и другими законами (например, «Кодекс об административных правонарушениях»).*
*В **ЮАР** — закон № 4 от 2013 г.: «Закон о защите персональной информации» от 2013 г.*
*В **Бразилии**, на данный момент, нет общего закона о защите данных. Тем не менее, есть ряд законов, таких как Билль о правах в интернете (Marco Civil da Internet), а также Кодекс защиты прав потребителей (Codigo de Defensa de Consumidor) которые регулируют различные аспекты конфиденциальности и защиты данных. Однако есть проект закона о защите данных, который обсуждается в бразильском конгрессе.*
*В **Китае** – Решение об усилении защиты сетевой информации от 28 декабря 2012 г.; Регламент службы занятости и кадровых отделов; Меры по наказанию за нарушение прав и интересов потребителей.*
*В **Объеденных Арабских Эмиратах** – отсутствует общее федеральное законодательство о защите персональных данных, аналогичное законам, применимым в Европе, хотя организации, принадлежащие Международному финансовому центру Дубая (DIFC), регулируются общими законами о защите данных.*

1.2.4. гарантировать, что каждая Компания Группы использует стандартную среду защиты Персональных данных, чтобы обеспечить возможность передачи Персональных данных между Компаниями Группы и гарантировать необходимую защиту Персональных данных в соответствии с применимым законодательством о международной передаче данных в случаях, когда они передаются через границу.

2. Сфера применения

2.1. Данная политика распространяется на:

2.1.1. все Компании Группы (в соответствии с определением, приведенным ниже) и их агентов;

2.1.2. всех Сотрудников, и;

2.1.3. все Персональные данные, собранные, хранящиеся и обрабатываемые Компаниями Группы в ходе их коммерческой деятельности, вне зависимости от носителя информации, на котором они записаны.

3. Определения

Приведенные ниже определения являются внутренними определениями, которые, сохраняя значение, предусмотренное применимым законодательством, могут иметь другое наименование в местном законодательстве. Разрабатывая местные процедуры, Регионы должны придерживаться терминологии и юридической концепции, используемой в соответствующем законодательстве их стран, обеспечивая при этом соответствие принципам настоящей Политики.

3.1. **Совет** — Совет Менеджеров Eurasian Resources Group SARL.

3.2. **Персональные данные клиентов** — Персональные данные, собранные в процессе обычного управления взаимоотношениями с клиентами, такие как контактная информация клиентов, их имена и рабочие адреса.

3.3. **Контролер Персональных данных** — физическое или юридическое лицо, государственный орган, агентство или иное учреждение, которое самостоятельно или совместно с другими определяет цели и способы обработки Персональных данных.

3.4. **Ответственный за защиту данных** – физическое лицо, которому поручено консультировать и проверять соблюдение Группой местного законодательства о защите данных, а также выполнять функции контактного лица для внутренних и внешних запросов Субъектов данных относительно сбора и обработки их Персональных данных

3.5. **Обработчик данных** — физическое или юридическое лицо (включая Компанию Группы), государственный орган, агентство или иное учреждение, которое обрабатывает Персональные данные от имени какой-либо Компании Группы.

3.6. **Субъект данных** — любое идентифицированное или идентифицируемое физическое лицо, к которому относятся Персональные данные.

3.7. **Сотрудники** — персонал любой Компании Группы, работающий на основе полной или частичной занятости или на временной основе, стажеры и подрядчики, работающие в помещениях или на площадках Компании Группы или имеющие доступ к ИТ-системам Компании Группы.

3.8. **Европейский союз –** 28 стран-участниц, которые формируют Европейский союз и на которые распространяется европейское законодательство.

3.9. Европейская экономическая зона (ЕЭЗ) - европейские страны, которые перенесли в свое национальное законодательство некоторые акты законодательства Европейского союза и согласились полностью соблюдать европейское законодательство, касающееся защиты Персональных данных.

3.10. Персональные данные сотрудников — Персональные данные, собранные в ходе обычного управления персоналом, например, имя, адрес, гражданство, пол, семейное положение, номер социального страхования и банковские реквизиты.

3.11. Общий регламент по защите данных – Регламент (ЕС) 2016/679 Европейского Парламента и Совета от 27 апреля 2016 г. «О защите физических лиц в отношении обработки Персональных данных и о свободном движении таких данных», а также Регламент 679/2018 – законодательный акт ЕС в сфере конфиденциальности и защиты Персональных данных, призванный гармонизировать правила в данной области. Данный регламент применяется во всех странах Европейского союза и ЕЭЗ и регулирует передачу и обработку Персональных данных Субъектов Персональных данных в ЕС и ЕЭЗ, независимо от того, совершаются ли такие действия на территории или за пределами Европейского союза или ЕЭЗ.

3.12. Компании Группы — Eurasian Resources Group SARL и любое предприятие, в котором она прямо или косвенно владеет более чем пятьюдесятью процентами (50%) голосующих прав, или в котором полномочия по контролю предприятия принадлежат Eurasian Resources Group SARL или лицу, действующему от ее имени.

3.13. Акционеры Компаний Группы – физические лица и (или) государственные либо частные компании, владеющие акциями Компаний Группы, которые предоставляют им права голоса.

3.14. Внешний представитель – лицо не из Компании Группы, назначенное Департаментом комплаенс для представления интересов офисов Компании Группы без участия Ответственного за защиту данных. Внешний представитель выступает в качестве контактного лица для вопросов относительно Персональных данных, поступающих от граждан и постоянных жителей ЕС и ЕЭЗ, которые постоянно или временно находятся за пределами стран ЕС или ЕЭЗ.

3.15. Персональные данные — любая информация любого рода, вне зависимости от типа ее носителя, включая звукозаписи и изображения, имеющая отношение к идентифицированному или идентифицируемому физическому лицу. Физическое лицо считается идентифицируемым, если его можно прямо или косвенно идентифицировать, в частности по идентификатору, например, по имени, идентификационному номеру, данным о местонахождении, идентификатору в сети Интернет или по одному, или нескольким параметрам, относящимся к его физическим, физиологическим, генетическим, интеллектуальным, культурным, социальным или экономическим характеристикам. Даже если сразу не очевидно, что лицо можно идентифицировать, оно все равно может быть идентифицируемым, если Компаниям Группы доступны или могут быть доступны приемлемые средства, позволяющие идентифицировать такое лицо.

3.16. Нарушение безопасности Персональных данных – нарушение безопасности, которое привело к случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию передаваемых, хранимых или обрабатываемых иными способами Персональных данных или к получению несанкционированного доступа к таким данным.

3.17. Обработка — любая операция или комплекс операций, которые осуществляются с Персональными данными с помощью автоматизированных или электронных средств или без таковых, например, сбор, запись, организация, хранение, адаптация или изменение, извлечение, обсуждение, использование, разглашение посредством передачи, распространения или предоставления иным образом, группирование или комбинирование, блокирование, удаление или уничтожение.

3.18. Регионы – группа из одной или нескольких Компаний Группы, расположенных в одной географической зоне. Регионами Группы являются Казахстан, Африка, Бразилия и Европа.

3.19. Особая категория Персональных данных — Персональные данные (как это определено в Общем регламенте Европейской комиссии по защите данных и актах местного законодательства стран, не входящих в ЕС), которые раскрывают физическое или психическое здоровье Субъекта данных, его религиозные или аналогичные верования, политические взгляды, расовое или этническое происхождение, членство в профсоюзах, уголовные преступления, сексуальную ориентацию, сексуальную жизнь и генетическую информацию.

3.20. Персональные данные Поставщиков — Персональные данные, собранные в процессе обычного управления взаимоотношениями с поставщиками, например, контактная информация поставщика, его имя и рабочий адрес.

4. Положения политики

4.1. Каждая Компания Группы обрабатывает Персональные данные в соответствии с применимыми законами и нормативными актами о защите данных.

4.2. Каждая Компания Группы и все бизнес-подразделения, вне зависимости от юрисдикции, должны соблюдать нижеуказанные минимальные нормы:

4.2.1. Добросовестная и законная Обработка Персональных данных: Компании Группы обрабатывают Персональные данные честным и законным образом, что требует, помимо прочего, следующего:

a) Законное использование: Персональные данные нельзя использовать способом, который может быть незаконным и/или оказывает неоправданное или непропорциональное отрицательное воздействие на Субъекта данных;

b) Прозрачность: Компании Группы должны обеспечить прозрачность процесса обработки данных для Субъектов данных (в частности, в отношении наличия такого Процесса и его условий);

c) Ограничение цели: Персональные данные должны собираться только для установленных и законных целей и использоваться только таким образом, который Субъект данных на разумных основаниях может ожидать; способ их обработки также должен соответствовать целям, для которых их собирали;

d) Соразмерность/минимизация объема данных: Персональные данные должны быть соразмерными, а также должны ограничиваться объемом, необходимым для целей, для которых осуществляется их Обработка;

e) Точность: Персональные данные должны быть точными и поддерживаться в актуальном состоянии;

f) Хранение: Персональные данные должны храниться в соответствии с требованиями соответствующих политик Группы и применимого законодательства, однако при этом они не должны храниться в форме, которая позволяет установить личность Субъекта данных, в течение более длительного времени, чем это необходимо для целей, в которых они обрабатываются. В принципе Персональные данные необходимо уничтожать или обезличивать, после того как цель, для которой осуществлялась их обработка, перестала существовать;

g) Соблюдение прав Субъектов данных: Каждая Компания Группы должна уважать и соблюдать законные права Субъектов данных в ходе обработки их Персональных данных.

4.2.2. Предварительное информирование и/или согласие: если этого требует местное законодательство, Компания Группы должна предоставить Субъектам данных необходимую основную информацию о Персональных данных, которые она собирает, и о том, как они будут обрабатываться[2], а также, если это необходимо согласно местному законодательству, получить на это четко выраженное и прямое согласие Субъекта данных. Данное согласие не может быть выражено в форме бездействия Субъекта данных или использования им графы документа, содержащей какую-либо отметку. Уведомления о конфиденциальности должны быть доступны Субъектам данных (например, опубликованы на веб-сайтах всех Компаний Группы или опубликованы с помощью других средств коммуникации).

4.2.3. Безопасность данных: Каждая Компания Группы должна принять надлежащие технические, физические и организационные меры, в том числе меры защиты против несанкционированной или незаконной Обработки Персональных данных, а также случайной утраты, случайного уничтожения или повреждения данных.

a) Информационная безопасность регулируется политиками и процедурами в области Информационной безопасности.

b) Каждая Компания Группы также несет ответственность за все действия по Обработке, выполняемые Обработчиками данных от имени данной Компании Группы. Компании Группы выполняют эту обязанность посредством детальной комплексной проверки потенциальных Обработчиков данных и включения особых условий и положений о защите данных в договоры с ними согласно требованиям нормативно-правовых актов в области защиты данных, в особенности статьи 28 Общего регламента по защите данных.

c) Сотрудники, которые желают привлечь Обработчика данных к обработке данных от имени Компании Группы, должны провести детальную комплексную проверку стандартов обработки данных Обработчика данных и обратиться к местному главному юрисконсульту и Ответственному за защиту данных в соответствующем Регионе, чтобы убедиться в том, что применяются подходящие договорные условия о защите данных, а также обеспечить соблюдение каждым Обработчиком данных требований нормативно-правовых актов в области защиты данных путем проведения анализа рисков, аудитов и проверок.

4.3. Каждый Регион должен определить представителя, ответственного за защиту данных из числа руководителей, который должен:

4.3.1. нести ответственность за локальное внедрение и соблюдение настоящей Политики и применимых законов и нормативных актов о защите данных;

4.3.2. нести ответственность за внедрение процедур в целях соблюдения настоящей Политики и применимых законов и нормативных актов о защите данных;

4.3.3. нести ответственность за взаимодействие с полномочными государственными органами в области защиты Персональных данных;

4.3.4. определить вместе с руководителями бизнес-единиц, вовлеченных в Обработку данных, цели и способы обработки Персональных данных каждой Компанией Группы, а также определить, соответствуют ли данные цели и способы местному законодательству;

4.3.5. организовать рассмотрение вопросов и проблем Сотрудников и Компаний Группы, связанных с внедрением и соблюдением настоящей Политики и применимых законов и нормативных актов о защите данных;

---

[2] *Например, в зависимости от применимых местных правил о защите данных, каждая Компания Группы может быть обязана сообщить Субъектам данных: (i) свои идентификационные данные или юридическое наименование; (ii) (в некоторых случаях) какие данные собираются или обрабатываются; (iii) для каких целей собираются данные; (iv) будут ли эти данные передаваться кому-либо еще; а также (v) их предусмотренные законодательством права и способ их осуществления.*

4.3.6. принимать вопросы или жалобы Субъектов данных относительно проблем, связанных с защитой данных и безопасностью данных, а также выполнять функции первичного контактного лица для запросов Субъектов данных, связанных с осуществлением ими своих законных прав;

4.4. Если не предусмотрено делегирование на региональном уровне, представителем, ответственным за защиту данных считается и соответствующие функции выполняет старший региональный Комплаенс-офицер или назначенное им лицо.

4.5. Руководители бизнес-единиц при содействии представителей, ответственных за защиту данных, должны внедрить надлежащие меры по защите данных, которые являются, как минимум, такими же строгими, как те, которые определены в настоящей Политике, или более строгими, и обеспечивают соблюдение их Сотрудниками настоящей Политики и применимого местного законодательства, касающегося защиты данных.

4.6. Сотрудники должны немедленно сообщить о любых случаях утечки данных, будь то подтвержденных или предполагаемых, Ответственному за защиту данных. В противном случае, будут приняты дисциплинарные меры вплоть до увольнения или прекращения договорных отношений.

4.7. Ответственный за защиту данных должен немедленно проинформировать местного главного юрисконсульта или Главного директора по юридическим вопросам Группы, Директора по комплаенс Группы, руководителя Департамента по рискам Группы и руководителя Департамента по информационной безопасности Группы о любых рисках, связанных с защитой данных, потенциальных проблемах в вопросах соответствия и Нарушениях безопасности Персональных данных.

4.8. Ответственный за защиту данных, независимо от мнения местного главного юрисконсульта или Главного директора по юридическим вопросам Группы, Директора по комплаенс Группы, руководителя Департамента по рискам Группы и руководителя Департамента по информационной безопасности Группы, а также членов Совета или других сотрудников Компании Группы, принимает окончательное решение об информировании местный орган власти по защите данных о Нарушении безопасности Персональных данных в течение 72 часов после обнаружения данного нарушения в соответствии с правилами политики.

4.9. Ответственный за защиту данных должен вести учет всех случаев Нарушения безопасности Персональных данных, включая действия, предпринимаемые для ограничения рисков, которые несет Компания Группы, контакты с местными государственными органами в области защиты Персональных данных, а также обоснование причины, по которой информация о Нарушении безопасности Персональных данных не была сообщена соответствующим национальным государственным органам в области защиты Персональных данных.

4.10. Каждая Компания Группы в ЕС, выполняющая функции Контролера Персональных данных или Обработчика данных, должна уведомлять Ответственного за защиту данных обо всех операциях по Обработке Персональных данных, как того требует действующее законодательство. При необходимости, Ответственный за защиту данных поручает сотрудникам провести Оценку воздействия на защиту данных, если они установят, что та или иная операция по Обработке с учетом характера, масштаба, контекста и целей обработки, по всей вероятности, создаст высокий риск для прав и свобод Субъектов данных.

5. Правила

Цели Обработки Персональных данных:

5.1. Компании Группы могут обрабатывать Персональные данные только для следующих целей:

Персональные данные сотрудников

5.1.1. Специалисты по работе с персоналом имеют право обрабатывать Персональные данные сотрудников для выполнения условий трудовых договоров/принятия необходимых мер до заключения договоров, в целях выполнения юридических обязательств или реализации законных интересов Компаний Группы (в случаях, разрешенных местным трудовым законодательством) в отношении:

a) управления (местным и международным) персоналом и группами персонала в разных юрисдикциях; обеспечения ротации персонала внутри Группы;

b) административного управления Сотрудниками, включая выполнения условий трудового договора и соблюдения социального, налогового и трудового законодательства и норм; а также

c) общего управления персоналом, включая подбор, наем, оплату труда, предоставление отпуска, обучение, оценку, анализ численности, планирование карьеры и преемственности руководящего персонала

d) информации, устанавливающей личность, включая имя, домашний адрес, дату рождения, пол, связанные с работой фотографии и номер домашнего телефона;

e) идентификационных номеров, присваиваемых государством, включая номер государственного удостоверения личности, для целей оплаты труда и управления доступом к информационным системам;

f) иммиграционного статуса, прав на работу и статуса проживания;

g) контактной информации на случай чрезвычайных ситуаций, а также информации о родственниках (в ограниченном объеме);

h) информацию, имеющую отношение к работе, включая, но не ограничиваясь – информацию о периодах занятости, месте работы, идентифицирующих данных сотрудника, рабочие записи, информацию об отпусках, а также контрактные данные;

i) информации об образовании и обучении, а также информации о найме на работу и эффективности работы, включая цели, оценки, комментарии, полученную обратную связь, опыт работы, рабочее оборудование, планирование карьеры и преемственности, навыки и компетенции и другие квалификации, связанные с работой;

j) информации об использовании ИТ-активов ERG;

k) информации, необходимой для управления комплаенс и рисками, включая информацию о взысканиях, результаты проверки биографии и данные в области безопасности, а также

l) информации об оплате труда и выплатах или льготах, включая информацию о заработной плате и страховании, налоговую информацию, банковские реквизиты и информацию о дополнительных выплатах и льготах для сотрудников.

5.1.2. Руководитель Сотрудника и высшее руководство, по мере необходимости, также вправе обрабатывать Персональные данные отдельного Сотрудника для выполнения обязательств, предусмотренных трудовыми договорами, или выполнения юридических обязательств и реализации законных интересов Компании Группы в отношении управления (местным и международным) персоналом и группами персонала в разных юрисдикциях; а также для администрирования, подбора, найма и оценки персонала и планирования преемственности руководящего персонала.

5.1.3. Бухгалтерский персонал вправе обрабатывать Персональные данные сотрудников в целях выполнения юридических обязательств Компаний Группы в отношении управления счетами, начисления заработной платы, премий, а также налогов и других вычетов, взносов и выплат.

5.1.4. Комитет по вознаграждениям вправе обрабатывать Персональные данные сотрудников для выполнения обязательств, предусмотренных трудовыми договорами, или исполнения юридических обязательств Компании Группы в целях определения размера оплаты труда сотрудника.

Персональные данные клиентов

5.1.5.Сотрудники могут обрабатывать Персональные данные клиентов только для поддержки управления взаимоотношениями с клиентами в целях выполнения договорных обязательств Компании Группы, обеспечения единого подхода к клиентам, а также управления договорами Компании Группы с клиентами (системы управления информацией о клиентах, CRM) для выполнения юридических обязательств или реализации законных интересов Компаний Группы.

Персональные данные поставщиков

5.1.6.Сотрудники могут обрабатывать Персональные данные поставщиков только для поддержки управления взаимоотношениями с поставщиками в целях выполнения договорных обязательств Компаний Группы, выполнения юридических обязательств и реализации законных интересов Компаний Группы в отношении удовлетворения ее потребностей в ресурсах, обеспечения единого подхода к поставщикам, а также управления договорами Компаний Группы с поставщиками.

Персональные данные акционеров

5.1.7.Корпоративные секретари каждой Компании Группы и назначенные сотрудники Юридической службы (определенные Главным директором по юридическим вопросам Группы) могут обрабатывать, хранить и использовать Персональные данные акционеров, их директоров, Совета, бенефициаров Группы, сотрудников и высшего руководства Компаний Группы, только если это необходимо соответствующей Компании Группы для соблюдения действующего законодательства и реализации интересов Группы, а также по другим законным деловым причинам.

5.1.8.Персональные данные акционеров Компании Группы, Совета и высшего руководства хранятся Корпоративным секретарем Группы в безопасном месте, доступ к которому может иметь только Корпоративный секретариат Группы и юридический представитель, утвержденный Главным директором по юридическим вопросам, при необходимой поддержке службы ИТ. Корпоративный секретарь подтверждает сотрудникам юридических служб (назначенным Главным директором по юридическим вопросам) любые изменения в этих Персональных данных раз в полгода или чаще, если Корпоративному секретарю станет известно о каких-либо изменениях.

5.1.9.Персональные данные Акционеров или совета для каждой из компаний Группы внутри отдельных регионов должны храниться соответствующим Корпоративным секретарем или местным главным юрисконсультом (или уполномоченным им сотрудником), в случае если Корпоративный секретарь не был назначен. Эти данные должны храниться в безопасном месте, доступ к которому может иметь только Корпоративный секретариат или Юридическая служба (в зависимости от обстоятельств) при необходимой поддержке службы ИТ. Региональный Корпоративный секретарь или местный главный юрисконсульт подтверждает любые изменения в этих Персональных данных раз в полгода или чаще, в случае если Корпоративному секретарю станет известно о таких изменениях. Эта информация должна быть предоставлена Корпоративному секретарю Группы раз в полгода после подтверждения любых изменений в Персональных данных.

5.1.10. Любые запросы на предоставление информации относительно конечных бенефициарных собственников (UBO) или любые иные запросы в рамках процедур «Знай своего клиента» (KYC)

касательно Акционеров Компании и правления каждой из компаний Группы, бенефициаров Группы и директоров, должностных лиц и высшего руководства компаний Группы, которые поступают в Группу, должны быть направлены Корпоративному секретарю Группы.

5.1.11. В случае если Корпоративный секретарь посчитает, что это необходимо в интересах Группы, он своевременно отвечает на запросы по установленной форме, используя информацию, хранящуюся в соответствии с пунктом 5.1.6, предоставляемую раз в полгода, или чаще, если Корпоративному Секретарю станет известно о любых изменениях или если он обратится к соответствующим Субъектам данных.

5.1.12. Раз в полгода Корпоративный секретарь должен уведомить акционеров и Совет об использовании этих данных.

5.1.13. Любые сотрудники Группы, которым Корпоративный секретарь считает необходимым оказать содействие в обработке, хранении и управлении Персональными данными акционеров и членов правления каждой компании Группы, бенефициаров Группы и директоров, должностных лиц и высшего руководства компаний Группы, должны подтвердить, что они ознакомлены с настоящей Политикой и будут соблюдать ее требования. Списки лиц, которые утверждены для работы с такими Персональными данными, хранятся Корпоративным секретарем. Списки лиц, которые составлены региональными Корпоративными секретарями или местными главными юрисконсультами (в зависимости от обстоятельств), в целях обработки, хранения и управления Персональными данными, связанными с компаниями Группы, управляемыми Регионами, ведутся региональными корпоративными секретарями или местными главными юрисконсультами (в зависимости от обстоятельств). Сотрудники, работающие или имеющие необходимость работать с такими Персональными данными, должны получить для этих целей одобрение своего непосредственного руководителя и уведомить Корпоративного секретаря Группы или Главного директора по юридическим вопросам, а также Руководителя компании или Региона (в зависимости от обстоятельств). Копии этих списков должны быть предоставлены Корпоративному секретарю Группы раз в полгода.

5.1.14. Главный исполнительный директор и Главный финансовый директор Группы вместе уполномочены разработать и утверждать любые дальнейшие внутренние процедуры, указания, наделение полномочиями и шаблоны, необходимые для обеспечения выполнения пунктов 5.1.6 - 5.1.13 включительно.

Особая категория Персональных данных

Только сотрудники по работе с персоналом и работающие на Компанию медицинские сотрудники (если применимо) имеют право обрабатывать Особую категорию Персональных данных для выполнения юридических обязанностей Компании Группы по подготовке ответов на запросы государственных органов и обеспечению охраны труда сотрудников Компании. До обработки Особой категории Персональных данных региональный Ответственный за защиту данных должен провести соответствующую проверку с тем, чтобы определить, повлияет ли обработка таких данных на права и свободы Субъекта Персональных данных.

5.1.15. Только следующие Особые категории Персональных данных могут обрабатываться Компаниями Группы:

a) религиозная принадлежность для целей налогообложения у источника выплаты[3];

b) медицинская документация[4].

3 *Относится, например, к Швейцарии.*

4 *Распространяется на те бизнес-подразделения, которые предоставляют услуги собственных медицинских специалистов, или которые проводят медицинские анализы или собирают их результаты (например, анализы на содержание алкоголя или наркотиков и т. д.).*

5.1.16.Сотрудники по работе с персоналом должны проводить такую обработку в соответствии с требованиями применимых нормативно-правовых актов.

5.1.17. Медицинская документация может обрабатываться только зарегистрированными медицинскими специалистами в соответствии с требованиями законодательства. Конфиденциальные

5.1.18. Персональные данные предоставляются Сотрудникам, только если это разрешено местным трудовым законодательством и законодательством в области защиты Персональных данных, и строго в соответствии с принципом служебной необходимости. Доступ к Особой категории Персональных данных могут получать только те Компании Группы, которые обязаны обрабатывать такие данные в соответствии с требованиями применимого местного законодательства.

Персональные ИТ-данные

5.1.19. Каждая Компания Группы может обрабатывать Персональные данные, связанные с использованием стандартной ИТ-системы, которая дает возможность сотрудникам и третьим лицам, в числе прочего, обмениваться электронными сообщениями, посещать веб-сайты в интернете, сохранять файлы и данные, использовать программные приложения, а также создавать, использовать и хранить сообщения диагностики и лог-файлы, если это требуется или разрешено в соответствии с действующим законодательством.

5.1.20. Если местное законодательство и нормы требуют получения разрешения (например, от органа регулирующего защиту данных, или другого местного органа) на обработку Персональных данных, указанных в пункте 5.1.19. (например, для ИТ-мониторинга Сотрудников), то Компания Группы должна своевременно получить такое разрешение.

5.1.21. В процессе обработки Персональных ИТ-данных Компании Группы должны соблюдать применимые нормы о неприкосновенности частной жизни, таких как тайна переписки или частной электронной корреспонденции.

Прочие Персональные данные

5.1.22. Сотрудники также могут обрабатывать Персональные данные в соответствии с политиками и процедурами информационной безопасности и Политикой приемлемого использования. Цель такой обработки и объем обрабатываемых данных подробно описаны в указанных политиках.

Прозрачность, информирование и права Субъектов Персональных данных

5.2. Большую часть Персональных данных, которые получают Компании Группы, предоставляет сам Субъект данных. При сборе Персональных данных каждому Субъекту данных, если того требует местное законодательство, необходимо сообщить следующую информацию[5]:

5.2.1. фирменное наименование Компании Группы (или Компаний Группы), которая(ые) собирает(ют) информацию как Контролер Персональных данных;

5.2.2. имена и контактные данные регионального представителя, ответственного за защиту данных или Внешнего представителя, к которым Субъект данных может обратиться по вопросам, связанным с его Персональными данными;

5.2.3.цель (цели) данной Обработки, а также ее юридическое основание

5.2.4.реализуемые при этом законные интересы (в тех случаях, когда это применимо);

5.2.5. Группа или получатели из числа третьих лиц (названные по отдельности или совместно с использованием родовых названий, например, «Компании Группы» или «местные органы

5 *Такая информация может быть частью договора, шаблона заявления о приеме на работу и т.д.*

власти»), которые получат Персональные данные для их обработки в своих независимых целях (во избежание неопределенности настоящим поясняется, что раскрывать информацию об Обработчиках данных Субъектам Персональных данных не обязательно);

5.2.6. Является ли Контролером Персональных данных лицо из ЕС или Швейцарии и, если это применимо, что Контролер Персональных данных планирует передать Персональные данные получателю, находящемуся за пределами Европейского союза/ЕЭЗ, а также:

- обеспечит ли данная третья страна достаточный уровень защиты Персональных данных согласно стандартам ЕС (т. е. имеется ли решение Европейской комиссии о достаточной защите) и (в случае отрицательного ответа),

- ссылка на соответствующие или подходящие меры защиты, принятые Контролером Персональных данных для обеспечения безопасности передачи, способ получения их копии или место их предоставления; а также

- имена и контактные данные регионального Ответственного за защиту данных или Внешнего представителя, к которому Субъект данных может обратиться по вопросам, связанным с его Персональными данными;

5.2.7. срок хранения Персональных данных или, если это невозможно, критерии, используемые для определения продолжительности данного срока;

5.2.8 Если Контролером Персональных данных является лицо из ЕС или Швейцарии, законные права Субъекта данных; например, в Европейском союзе к данным правам относится:

- право запрашивать доступ к Персональным данным, право на их уточнение или удаление;

- право требовать ограничения Обработки применительно к Субъекту данных (при соблюдении определенных условий);

- право возражать против Обработки (при соблюдении определенных условий). Субъекты Персональных данных имеют право в любой момент представить возражение против обработки своих Персональных данных на убедительных законных основаниях, связанных с их ситуацией, кроме случаев, когда такая обработка данных требуется в соответствии с законодательством. Они имеют право на безвозмездной основе представить возражение против обработки Персональных данных для целей прямого маркетинга;

- право переносить Персональные данные на другие платформы, а также

- право подать жалобу в уполномоченные государственные органы по защите данных.

5.2.9. Если Персональные данные получены от третьего лица, Компании Группы должны в течение разумного срока после получения Персональных данных, но не позднее, чем через месяц, учитывая конкретные обстоятельства обработки Персональных данных, проинформировать Субъекта данных о соответствующих категориях Персональных данных, источнике, из которого они получены, и, в тех случаях, когда это применимо, о том, что данные получены из общедоступных источников.

Однако обязательство уведомить Субъекта данных в таком случае может не быть применимым, если Субъект данных уже имеет соответствующую информацию.

5.2.10. Запросы Субъектов данных, касающиеся их прав, следует направлять региональному Ответственному за защиту данных. Ответ должен быть направлен Субъектам данных в течение одного месяца. Однако, если запрос является сложным или Компании Группы получают большое количество запросов, этот срок может быть дополнительно продлен на два месяца.

Автоматизированные решения[6]

5.3. Оценка Субъекта данных или решения в отношении него, которые существенно влияют на него, не могут быть основаны исключительно на автоматизированной/электронной обработке Персональных данных, за исключением случаев, когда такое решение:

5.3.1. принимается в процессе заключения или исполнения договора, при условии, что запрос, поданный Субъектом данных, удовлетворен, или приняты соответствующие меры для защиты законных интересов Субъекта данных, такие, как договоренности, позволяющие Субъекту данных высказать свою точку зрения; или

5.3.2. разрешено законом, который также предусматривает меры, защищающие законные интересы Субъекта данных.

Субъекты данных имеют право требовать участия человека в любой автоматизированной обработке данных.

Хранение данных

5.4. Сотрудники должны хранить Персональные данные, как в электронной форме, так и на бумажном носителе согласно соответствующим политикам Компании Группы, а также в соответствующих случаях графику хранения, утвержденному Главным исполнительным директором Группы. Главный исполнительный директор уполномочен Советом принимать и вносить изменения в график хранения по предложению главного юрисконсульта, но по согласованию с Ответственным за защиту данных.

Безопасность и конфиденциальность

5.5. В соответствии с требованиями Политик и процедур информационной безопасности в каждой Компании Группы должны быть внедрены и применяться надлежащие технические и организационные меры для защиты Персональных данных от случайного или незаконного уничтожения, случайной утраты, изменения или несанкционированного разглашения, или доступа.

5.6. В случае случайного или незаконного уничтожения, или случайной утраты, изменения или несанкционированного разглашения Персональных данных или доступа к ним, Компании Группы должны следовать процедурам, предусмотренным применимым законодательством о защите данных, политикам и процедурам Компании Группы, а также указаниям компетентных органов по защите данных. В случае, если в качестве Обработчика данных выступает Компания Группы в ЕС:

- выполняя функции Обработчика данных, она должна сообщить Контролеру Персональных данных об утечке Персональных данных незамедлительно после обнаружения данного нарушения, а также

- выполняя функции Контролера персональных данных, если, по мнению Ответственного за защиту данных, это необходимо, Ответственный за защиту данных должен уведомить об утечке Персональных данных компетентный местный орган власти по защите данных без неоправданной задержки и по возможности в течение 72 часов после обнаружения данного нарушения. Такое уведомление должно включать всю информацию, требуемую в соответствии с действующим законодательством о защите данных. Кроме того, если утечка Персональных данных, по всей вероятности, создаст высокий риск для прав и свобод Субъекта данных, Контролер Персональных данных должен сообщить об утечке Персональных данных соответствующим Субъектам данных

[6] *В число примеров автоматизированных решений входит автоматизированный анализ первичных тендерных/конкурсных заявок или автоматизированный анализ анкет кандидатов на трудоустройство.*

без неоправданной задержки, за исключением случаев, когда может быть документально подтверждено, что применяется установленное законодательством освобождение.

Передача Персональных данных внутри Группы Компаний

5.7. ERG является международной компанией, и ей периодически требуется передавать Персональные данные между своими аффилированными и дочерними компаниями.

5.8. Персональные данные могут быть предоставлены другим Компаниям Группы только в соответствии с настоящей Политикой. Персональные данные защищены при обработке любой Компанией Группы посредством соблюдения общих строгих организационных и технических мер безопасности, предусмотренных политиками и процедурами информационной безопасности, и настоящей Политикой.

5.9. Чтобы обеспечить возможную передачу Персональных данных между Компаниями Группы, следует использовать стандартные пункты договоров.

Передача Персональных данных Обработчикам данных

Передача Персональных данных Компаниями Группы, расположенными в ЕС, Обработчикам данных, расположенным в пределах ЕС либо в ассоциированных странах

5.10. Если Компания Группы, находящаяся в ЕС, желает передать Персональные данные Обработчику данных, расположенному в ЕС, ЕЭЗ или в стране, которая признается Европейской комиссией как гарантирующая адекватный уровень защиты[7], перед передачей данных необходимо выполнить следующее:

5.10.1. заключить письменный договор между Компанией Группы и Обработчиком данных; и

5.10.2. данный договор должен быть основан на образце Соглашения об обработке Персональных данных (или содержать равноценные условия), утвержденном Группой и имеющемся у Ответственного за защиту данных в Европе.

Передача Персональных данных Компаниями Группы, расположенными в ЕС, Обработчикам данных, расположенным за пределами ЕС или ассоциированных стран

5.11. Если Компания Группы, находящаяся в ЕС, желает передать Персональные данные Обработчику данных, расположенному за пределами ЕС, ЕЭЗ или в стране, которая не признается Европейской комиссией как гарантирующая адекватный уровень защиты, ответственный Сотрудник должен убедиться в следующем:

5.11.1. что такая передача осуществляется в соответствии с положениями обязательного Внутригруппового соглашения;

5.11.2. при отсутствии такого Внутригруппового соглашения Компании Группы должны заключить письменный договор, который основан на образце Соглашения об обработке Персональных данных (или содержит равноценные условия), утвержденном Группой и имеющемся у юридического подразделения Группы;

[7] *Европейская комиссия на текущий момент признала, что адекватную защиту обеспечивают Андорра, Аргентина, Австралия, Канада (коммерческие организации), Швейцария, Фарерские острова, Гернси, Израиль, остров Мэн, Джерси, Новая Зеландия и Уругвай. (См. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm для получения актуальной информации).*

5.11.3. любая передача Персональных данных должна быть защищенной и осуществляться в соответствии с применимым законодательством в отношении международной передачи данных;

5.11.4. соответствующая Компания Группы, передающая Персональные данные, должна была (i) до передачи Персональных данных заключить с Обработчиком данных договор, включающий ряд стандартных условий в форме, одобренной Европейской комиссией; и (II) выполнить необходимые формальности и подать необходимые документы в соответствии с местным законодательством.

Передача Персональных данных Компаниями Группы, расположенными за пределами ЕС

5.12. Если Компания Группы, расположенная за пределами ЕС, желает передать Персональные данные Обработчику данных, расположенному за пределами ее страны регистрации, местный главный юрисконсульт должен убедиться, что передача ведется в полном соответствии с местными законами и нормативными актами, регулирующими защиту данных и международную передачу Персональных данных.

Персональные данные сотрудников, увольняющихся из Компании Группы

5.13. В случае увольнения сотрудника из Компании Группы данная Компания должна осуществить следующее:

5.13.1. предоставить каждому увольняющемуся сотруднику возможность сделать копии своих Персональных данных, хранящихся в ящиках входящих сообщений его электронной почты, а также на корпоративных компьютерах и мобильных вычислительных устройствах.

5.13.2. в возможно кратчайшие сроки после увольнения сотрудника деактивировать его корпоративный адрес электронной почты.

Программа обучения

5.14. Все сотрудники, которые имеют постоянный и (или) регулярный доступ к Персональным данным, должны на периодической основе проходить обучение по сбору и обработке Персональных данных или по разработке инструментов, используемых для обработки Персональных данных.

5.15. Все прочие сотрудники должны пройти обучение по настоящей Политике после приема на работу в Компанию и, по мере необходимости, в дальнейшем.

6. Работа с вопросами, проблемами и запросами

6.1. При возникновении у Сотрудника вопросов или сложностей, связанных с защитой данных, ему необходимо обратиться к Ответственному за защиту данных.

6.2. Если какой-либо Субъект данных считает, что его данные обрабатываются с нарушением настоящей Политики, он должен сообщить о своей проблеме соответствующему Ответственному за защиту данных.

6.3. Если Сотрудник получит жалобу от Субъекта данных, не входящего в группу, он должен незамедлительно направить ее соответствующему Ответственному за защиту данных.

6.4. Ответственный за защиту данных должен рассмотреть жалобу на конфиденциальной основе. В случае если Ответственный за защиту данных недоступен, местный главный юрисконсульт рассмотрит и направит жалобу Ответственному за защиту данных, как только он или она будет доступен (доступна).

6.5. Компании Группы, уведомив регионального Ответственного за защиту данных, должны незамедлительно инициировать расследование по любому обращению о нарушении настоящей Политики.

6.6. Сотрудники обязаны оказывать содействие в проведении внутренних расследований, относящихся к возможным нарушениям Политики.

6.7. Чтобы Группа могла надлежащим образом провести расследование, обращение о несоблюдении или нарушении Политики должно содержать достаточную информацию об инциденте или нарушении.

6.8. Группа обеспечивает конфиденциальность лица, направившего жалобу. Однако в определенных обстоятельствах Группа может быть обязана по закону сообщить информацию или сведения о лице, направившем жалобу или обращение.

6.9. Соответствующий Ответственный за защиту данных должен хранить каждую жалобу и любые сведения, связанные с ней, в письменной и/или электронной форме до завершения рассмотрения жалобы или до иного момента, предусмотренного законом и политиками Компании Группы.

7. Ответственность

7.1. Совет отвечает за принятие настоящей Политики.

7.2. Служба комплаенс в соответствующем Регионе отвечает за:

7.2.1. Предоставление рекомендаций и консультирование Регионального руководства по вопросам внедрения настоящей Политики, а также контроль внедрения настоящей Политики;

7.2.2. Мониторинг соблюдения настоящей Политики;

7.2.3. Требования к предоставлению отчетности: предоставление периодических отчетов о статусе внедрения и соблюдения требований настоящей Политики.

7.3. Региональное руководство несет ответственность за эффективное внедрение настоящей Политики в своих соответствующих сферах ответственности и внедрение надлежащих механизмов контроля для обеспечения ее постоянного соблюдения.

7.4. Региональное руководство обязано назначить Ответственного за защиту данных, а также утвердить и обеспечить исполнение в своем Регионе политик и процедур, разработанных Ответственным за защиту данных.

7.5. Ответственные за защиту данных обязаны внедрить соответствующие процедуры, распределение обязанностей, обучение и внутренние механизмы контроля в своих Регионах, чтобы обеспечить последовательное внедрение настоящей Политики и соблюдение ее требований.

7.6. Региональное руководство обязано гарантировать, что соответствующие Сотрудники и используемые Обработчики данных ознакомлены с настоящей Политикой, и что сотрудники, обрабатывающие Персональные данные или имеющие к ним доступ, периодически проходят тренинги по требованиям к защите данных.

8. Мониторинг

8.1. Главный директор по юридическим вопросам и Ответственный за защиту данных должны на ежегодной основе предоставлять в Комитет по Комплаенс при Совете отчеты о соблюдении настоящей Политики. Региональные службы комплаенс должны ежегодно представлять отчеты о соблюдении настоящей Политики Главному директору по юридическим вопросам.

8.2. Внутренний аудит должен периодически проводить проверки соблюдения настоящей Политики и сообщать о любых недостатках и предоставлять соответствующие рекомендации Руководству Группы и Комитету по Комплаенс при Совете.

9. Несоблюдение Политики

9.1. Любые случаи несоблюдения Политики должны документироваться, и о них следует сообщать Ответственному за защиту данных, в Департамент комплаенс или по Горячей линии ERG.

9.2. Каждый Сотрудник компании обязан соблюдать положения настоящей Политики. В отношении сотрудников, нарушающих настоящую Политику, могут быть приняты дисциплинарные меры, предусмотренные местным законодательством, вплоть до увольнения.

10. Процесс пересмотра

10.1. Настоящая Политика ERG будет периодически (но не реже, чем раз в 2 года) обновляться с целью отражения любых изменений правовой и технологической среды, а также бизнес-требований.

10.2. Все запросы о внесении изменений следует направлять одному из владельцев Политики или контактным лицам.

10.3. Существенные изменения, вносимые в настоящую Политику ERG, должны утверждаться Советом или (в случае Приложения А) Главным исполнительным директором.

10.4 Настоящая политика ERG (в редакции 4.0) вступает в силу с 25 мая 2018 года.

Версия	Дата последнего изменения	Утверждено	Дата утверждения	Комментарии
1.0	24.08.2014	Советом	24.08.2014	
1.0	05.05.2015	Комплаенс	05.05.2015	
2.0	04.03.2016	Советом	13.03.2016	
3.0	20.08.2017	Советом	27.08.2017	
4.0	02.06.2018	Советом	02.06.2018	