ПОЛИТИКА ограниченного партнерства ООО «ГЕЛИОС» в отношении обработки персональных данных

ООО «Гелиос», именуемое в дальнейшем – «Компания» устанавливает политику Компании в отношении обработки персональных данных (далее – «Политика Компании»): - физических лиц, в том числе являющихся индивидуальными предпринимателями; - физических лиц – бенефициарных владельцев юридических лиц, либо таких, которые имеют возможность контролировать действия юридических лиц; - физического лица, являющегося бенефициарными владельцем физического лица, за исключением случаев, если имеются основания полагать, что бенефициарным владельцем является иное физическое лицо. Вышеуказанные лица в целях настоящей Политики Компании именуются в дальнейшем «Контрагенты» и каждое из них в отдельности – «Контрагент». «Компания» и «Контрагент», включая представителей каждого из них в целях настоящей Политики Компании именуются в дальнейшем «Партнеры».

Общие положения

1. Настоящая Политика Компании регулирует отношения между Компанией и Контрагентами в связи с обработкой их персональных данных, содержащихся в документарных и (или) бездокументарных (электронных) базах данных с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях (в том числе сети «Интернет»), или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

2. Настоящая Политика Компании распространяется на Контрагентов Компании и (или) других Контрагентов, а также их представителей.

3. Политика Компании направлена на обеспечение защиты прав и свобод Партнеров при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну каждого из них, а также конфиденциальность данной информации.

4. Настоящая Политика Компании распространяется на случаи, когда обработка персональных данных Контрагентов, Партнеров, позволяет им при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. В этом случае в отношении персональных данных вводится режим их конфиденциальности, на который распространяется законодательство о коммерческой тайне.

5. Настоящая Политика Компании распространяется на случаи обработки персональных данных, входящих в состав инсайдерской информации, а также в случае, если Оператор персональных данных является инсайдером. Политика Компании действует в части, не противоречащей законодательству и иным правовым актам, регулирующим порядок предоставления и распространения инсайдерской информации.

Основные понятия

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) или его представителю, содержащаяся в документарных и (или) бездокументарных (электронных) базах данных. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых в информационной системе с использованием средств автоматизации (обработка персональных данных с помощью средств вычислительной техники) или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу. Оператор персональных данных – Компания, ее Контрагенты, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных , подлежащих обработке, действия (операции), совершаемые с персональными данными. Оператором персональных данных может быть лицо, которому Компания поручает обработку персональных данных на основании заключаемого с этим лицом договора. Операторами персональных данных не могут быть Контрагент и его физические лица, а также

третьи лица, которые осуществили неправомерный или случайный доступ к персональным данным, несмотря на осуществление ими обработки персональных данных. Контрагенты Партнеров – физические лица, в том числе индивидуальные предприниматели, состоящие с Компанией в правоотношениях на основании заключенных трудовых договоров и договоров гражданско-правового характера, их представители, а также физические лица, указанные в абзацах третьем и четвертом преамбулы настоящей Политики Компании. Актуальные угрозы безопасности персональных данных – совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе с использованием средств автоматизации, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Обработка персональных данных

1. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

2. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3. В соответствии с Политикой Компании обработка персональных данных необходима в целях:

• защиты жизни, здоровья или иных жизненно важных интересов персональных данных Контрагентов Партнеров, если получение их согласия данных невозможно;

• исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является Компания или Контрагент, в том числе в случае реализации Компанией своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе Компании или Контрагента, или договора, по которому Компания или Контрагент будет являться выгодоприобретателем или поручителем;

• опубликования или обязательного раскрытия персональных данных Контрагентов Партнеров в соответствии с законодательством;

• продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальными Контрагентами с помощью средств связи.

4. Обработка персональных данных должна осуществляться на законной и справедливой основе.

5. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор персональных данных должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных, или неточных данных.

7. Хранение персональных данных осуществляется Компанией, а также лицами, указанными в частях 5 и 6 статьи V Политики Компании, в документарной и (или) электронной формах, в течение срока, который составляет не менее 5 лет. Более продолжительный срок хранения персональных данных может быть установлен в договорах, стороной которых, выгодоприобретателем или поручителем, по которым является Контрагент.

8. Обработка персональных данных Контрагентов Партнеров осуществляется с их согласия на обработку таких персональных данных, за исключением случаев, предусмотренных законодательством и настоящей Политикой Компании.

9. Контрагенты Компании выражают согласие на обработку их персональных данных Оператором персональных данных, за исключением иных Контрагентов и их физических лиц, а также третьих лиц в результате их неправомерного или случайного доступа к персональным данным.

10. Оператор персональных данных, осуществляющий обработку персональных данных по поручению Компании, не обязан получать согласие Контрагентов на обработку их персональных данных.

11. В случае, если Компания поручает обработку персональных данных другому Оператору персональных данных, ответственность перед Контрагентами за действия указанного лица несет Компания. Оператор персональных данных, осуществляющий обработку персональных данных по поручению Компании, несет ответственность перед Компанией.

Оператор персональных данных, ответственный за организацию обработки персональных данных, в частности, обязан:

• осуществлять внутренний контроль за соблюдением им и его работниками законодательства о персональных данных, в том числе требований к защите персональных данных;

• доводить до сведения работников Оператора персональных данных положения законодательства о персональных данных, международных правовых актов, настоящей Политики Компании по вопросам обработки персональных данных, требований к защите персональных данных;

• организовывать прием и обработку обращений и запросов Контрагентов или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;

• не передавать иным лицам исполнение принятых на себя обязательств в какой бы то ни было форме.

12. Контрагент и его физические лица, а также третьи лица, которые в результате неправомерного или случайного доступа к персональным данным, могут осуществить их обработку, несут юридическую ответственность перед Компанией и (или) Оператором персональных данных.

Трансграничная передача персональных данных

1. Компания выступает резидентом государства, не являющегося стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав Контрагентов Партнеров, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

2. Трансграничная передача персональных данных в целях настоящей Политики Компании осуществляется в случаях исполнения договора, стороной которого является Контрагент, а также для защиты жизни, здоровья, иных жизненно важных интересов Контрагента или третьих лиц при невозможности получения согласия в письменной форме Контрагента в случаях, предусмотренных законодательством и настоящей Политикой Компании.

3. До начала осуществления трансграничной передачи персональных данных и в процессе их последующей обработки Компания гарантирует адекватную защиту прав Контрагентов посредством осуществления следующих действий:

• определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

• применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает уровни защищенности персональных данных;

• применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

• оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

• учетом машинных носителей персональных данных;

• обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по устранению указанных нарушений;

• восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

• установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

• контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

4. Действие настоящей статьи распространяется на Контрагентов Партнеров в случае правомерной трансграничной передачи ими персональных данных. Контрагенты Партнеров гарантируют и принимают надлежащие меры безопасности, направленные на предотвращение случайного или несанкционированного уничтожения персональных данных, или их случайной потери, а также на предотвращение несанкционированного доступа к ним,

изменения или распространения таких данных в соответствии с данными требованиями, установленными в национальном законодательстве и предусмотренными Конвенцией о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 года (далее – «Конвенция»), принимая во внимание участие государств – членов Совета Европы, подписавших данную Конвенцию. В случае, если государство-резидент не является стороной Конвенции, Контрагенты Партнеров соблюдают требования настоящей Политики Компании.

Передача персональных данных

1. При передаче персональных данных Контрагентов Партнеров, если иное не предусмотрено Политикой Компании, должны соблюдаться следующие требования:

2. Запрещено сообщать персональные данные третьим лицам за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Контрагентов, Контрагентов Партнеров, а также в случаях, установленных законодательством.

В целях настоящего пункта под третьими лицами понимаются любые физические и юридические лица, с которыми Контрагенты, Контрагенты Партнеров могут вступать в правоотношения как на договорной, так и на бездоговорной основе.

3. Запрещено сообщать персональные данные Контрагентов, Контрагентов Партнеров в каких бы то ни было целях, не соответствующих целям настоящей Политики Компании.

4. Оператор персональных данных обязан предупредить Контрагентов, Контрагентов Партнеров, получивших персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц письменное подтверждение (либо подтверждение, сделанное в электронном виде) того, что это правило соблюдено. Лица, получившие персональные данные, обязаны соблюдать режим их конфиденциальности.

5. Оператор персональных данных обязан назначить должностное лицо (работника), ответственное за обеспечение безопасности персональных данных в информационной системе. Должностное лицо (работник) обязан осуществлять контроль за передачей только тех персональных данных, которые необходимы для выполнения конкретной функции и в целях, предусмотренных политикой Компании.

6. Персональные данные хранятся в подразделении безопасности и хранения персональных данных, созданном Контрагентами Партнеров. В случае отсутствия такого подразделения, Контрагент может заключить договор с иным Контрагентом – юридическим лицом, в котором создано такое подразделение на хранение персональных данных с обязательным ознакомлением под расписку с настоящей Политикой Компании.

7. Персональные данные могут быть получены, проходить дальнейшую обработку и передаваться на хранение как в документарной форме, так и в электронном виде.

Доступ к персональным данным

Право доступа к персональным данным Контрагентов Партнеров имеют:

• Контрагенты Партнеров в отношении своих персональных данных.

• Оператор персональных данных.

• Юридическое лицо, в котором создано подразделение безопасности и хранения персональных данных, с которым Контрагенты Партнеров могут заключить соответствующий договор.

Безопасность персональных данных

1. Помимо осуществления действий, предусмотренных в части 3 статьи IV настоящей Политики Компании, лица, ответственные за обработку персональных данных, обязаны принять все необходимые меры противодействия актуальным угрозам безопасности персональных данных:

• несанкционированному доступу к персональным данным Контрагентами, Контрагентами Партнеров, обладающими полномочиями в информационной системе персональных данных, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационной системы персональных данных;

• воздействию вредоносного кода, внешнего по отношению к информационной системе персональных данных;

• использованию методов социального инжиниринга к Контрагентам, Контрагентам Партнеров, обладающим полномочиями в информационной системе персональных данных;

• несанкционированному доступу к отчуждаемым носителям персональных данных;

• утрате (потере) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных;

• несанкционированному доступу к персональным данным, находящимся в информационной системе персональных данных, с использованием уязвимостей в организации защиты персональных данных;

• несанкционированному доступу к персональным данным, находящимся в информационной системе персональных данных, с использованием уязвимостей в программном обеспечении информационной системы персональных данных;

• несанкционированному доступу к персональным данным, находящимся в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;

• несанкционированному доступу к персональным данным, находящимся в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных;

• несанкционированному доступу к персональным данным, находящимся в информационной системе персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации.

2. Актуальные угрозы безопасности персональных данных подразделяются на 3 типа и должны приниматься во внимание лицами ответственными за обработку персональных данных при осуществлении ими мер безопасности:

• Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (не декларированных) возможностей в системном программном обеспечении, используемом в информационной системе;

• Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (не декларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе;

• Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (не декларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

3. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных:

а) Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

• для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

• для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора персональных данных.

б) Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

• для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

• для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников Оператора персональных данных или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора персональных данных;

• для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

• для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора персональных данных;

• для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора персональных данных;

• для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора персональных данных.

в) Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

• для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников Оператора персональных данных или общедоступные персональные данные менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора персональных данных;

• для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора персональных данных или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора персональных данных;

• для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников Оператора персональных данных или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора персональных данных;

• для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

• для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора персональных данных.

г) Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

• для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

• для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора персональных данных или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора персональных данных.

4. Для обеспечения безопасности всех уровней защищенности персональных данных, помимо обязанностей, предусмотренных частями 5 и 6 статьи V, необходимо выполнение дополнительных условий:

• автоматическая регистрация в электронном журнале безопасности возникновения, изменения и прекращения полномочий лиц, указанных в статье VI по доступу к персональным данным, содержащимся в информационной системе;

• доступ к содержанию электронного журнала безопасности был возможен исключительно для лиц, указанных в статье VI и строго в целях, предусмотренных Политикой Компании.

• обеспечение сохранности носителей персональных данных;

• организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

5. В случае выявления неправомерной обработки персональных данных при обращении Контрагентов, Контрагентов Партнеров Оператор персональных данных обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к Контрагентам, Контрагентам Партнеров, или обеспечить их блокирование с момента такого обращения. В случае выявления неточных персональных данных при обращении Контрагентов, Контрагентов Партнеров или их представителей Оператор персональных данных обязан осуществить блокирование персональных данных, относящихся Контрагентам, Контрагентам Партнеров, или обеспечить их блокирование с момента такого

обращения, если блокирование персональных данных не нарушает права и законные интересы Контрагентов, Контрагентов Партнеров или иных лиц.

6. В случае подтверждения факта неточности персональных данных Оператор персональных данных на основании сведений, представленных Контрагентами, Контрагентами Партнеров или их представителями, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

7. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или Контрагентами, Контрагентами Партнеров, а также третьими лицами, указанные лица в срок, не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, указанные лица в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных указанные лица обязаны уведомить Компанию, Контрагентов, Контрагентов Партнеров или их представителей.

8. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в части 4 настоящей статьи, Оператор персональных данных осуществляет блокирование таких персональных данных или обеспечивает их блокирование и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен законодательством.

9. В случае достижения цели обработки персональных данных Оператор персональных данных обязан прекратить обработку персональных данных или обеспечить ее прекращение и уничтожить персональные данные или обеспечить их уничтожение не ранее срока, предусмотренного в части 7 статьи III Политики Компании либо если Оператор персональных данных не вправе осуществлять обработку персональных данных без согласия Контрагентов, Контрагентов Партнеров, предусмотренных настоящей политикой Компании и (или) законодательством.

10. В случае отзыва Контрагентами, Контрагентами Партнеров согласия на обработку их персональных данных Оператор персональных данных обязан

прекратить их обработку или обеспечить прекращение такой обработки и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение не ранее срока, предусмотренного в части 7 статьи III Политики Компании либо если Оператор персональных данных не вправе осуществлять обработку персональных данных без согласия Контрагентов, Контрагентов Партнеров, предусмотренных настоящей политикой Компании и (или) законодательством.

Отзыв Контрагентами, Контрагентами Партнеров согласия на обработку их персональных данных может быть направлен Оператору персональных данных в письменной форме лично или их представителем, либо посредством электронной связи.

Конфиденциальность персональных данных

1. Оператор персональных данных обеспечивает условия конфиденциальности и сохранности материальных носителей персональных данных, исключающие несанкционированный доступ к ним с момента создания данных документов до истечения сроков их хранения и уничтожения.

2. Обязанность, предусмотренная в части 1 настоящей статьи, возникает у всех иных лиц, прямо или косвенно получивших доступ к персональным данным, включая информацию, предусмотренную в части 4 статьи I.

3. В целях защиты конфиденциальности персональных данных, Компания окажет всю необходимую правовую помощь и содействие Контрагенту, Контрагентам Партнеров, включая обращение в уполномоченные органы и организации стран-резидентов, международные организации и к должностным лицам, осуществляющим деятельность в сфере финансовых рынков, а также в саморегулируемые организации участников гражданско-правового сообщества.

Ответственность за нарушение Политики Компании

Оператор персональных данных, Контрагенты, Партнеры, Контрагенты Партнеров, а также третьи лица в результате их неправомерного или случайного доступа к персональным данным, несут юридическую ответственность в соответствии с законодательством.

Допустимые исключения

Настоящая Политика Компании предусматривает допустимые исключения, не противоречащие законодательству:

• предусмотренные в части 10 статьи 3;

• оператор персональных данных освобождается от обязанности предоставить Контрагентам, Контрагентам Партнеров сведения о наименовании либо фамилии, имени, отчестве и адресе Оператора персональных данных или его представителе;

• о цели обработки персональных данных и ее правовом основании;

• о предполагаемых пользователях персональных данных;

• об установленных настоящим правах Контрагентов, Контрагентов Партнеров;

• об источнике получения персональных данных в случаях, если персональные данные получены Оператором персональных данных на основании законодательства или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является Контрагент, Контрагенты Партнеров;

• иные исключения, предусмотренные законодательством.

Согласие Контрагента с Политикой Компании. Согласие Контрагента на обработку его персональных данных

1. Контрагент внимательно ознакомился с Политикой Компании, понимает ее смысл и содержание, в том числе специальные термины и определения и выражает согласие с Политикой Компании.

2. Контрагент обязуется соблюдать Политику Компании в полном объеме и, в случае ее несоблюдения в полном объеме или в части, несет установленную законодательством юридическую ответственность, в том числе за действия всех иных лиц, предусмотренные Политикой Компании.

3. Контрагент выражает согласие на обработку его персональных данных свободно, своей волей и в своем интересе, и в строго установленных целях обработки таких персональных данных.

* Цель обработки персональных данных (см.: часть 3 статьи III) – КОД: 3/III.

** Перечень персональных данных, на обработку которых дается согласие: данные, содержащиеся в документе, удостоверяющем личность Контрагента, сведения о профессии, абонентский номер, сведения об участии в органах управления в хозяйственных товариществах и обществах, размерах долей (паев, акций) и любые иные персональные данные, в том числе содержащиеся в договорах, выгодоприобретателем или поручителем, по которому является Контрагент – КОД: ППД-1.

*** В случае отсутствия указывается прочерк.

**** См.: часть 2 статьи II, статьи III, IV, V, VII – КОД: 2/II-ЕТС.

***** См.: часть 10 статьи VII – КОД: 10/VII.

В случае недееспособности Контрагента - физического лица согласие на обработку его персональных данных дает законный представитель Контрагента - физического лица.

В случае смерти Контрагента - физического лица согласие на обработку его персональных данных дают наследники Контрагента — физического лица, если такое согласие не было дано Контрагента — физическим лицом при его жизни.

В случае реорганизации Контрагента - юридического лица согласие на обработку его персональных данных дают его правопреемники - физические лица – бенефициарные владельцы реорганизованного Контрагента, либо такие, которые имеют возможность контролировать действия реорганизованного Контрагента; физического лица, являющегося бенефициарными владельцем физического лица, за исключением случаев, если имеются основания полагать, что бенефициарным владельцем является иное физическое лицо.

Персональные данные могут быть получены Компанией от лица, не являющегося Контрагента, при условии предоставления Компании подтверждения наличия оснований, предусмотренных законодательством.