

Утверждена
Приказом Генерального директора
ЗАО «Водоканал»
№ 24-АДМ от 20.06.2017г.



Политика

В части обработки и защиты персональных данных в
ЗАО «Водоканал».

1. Общие положения

1.1. Политика в отношении обработки персональных данных ЗАО «Водоканал» (далее - Политика) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», а также в соответствии с иными федеральными законами Российской Федерации, определяющими случаи и особенности обработки персональных данных и обеспечения безопасности и конфиденциальности такой информации (далее - Законодательство о персональных данных).

1.2. Политика устанавливает:

- цели обработки персональных данных;
- классификацию персональных данных и Субъектов персональных данных;
- общие принципы обработки персональных данных;
- основных участников системы управления процессом обработки персональных данных;
- основные подходы к системе управления процессом обработки персональных данных.

1.3. Положения настоящей Политики являются основой для организации работы по обработке персональных данных в Организации, в том числе, для разработки иных внутренних нормативных документов, регламентирующих порядок и процессы обработки персональных данных.

1.4. Положения настоящей Политики являются обязательными для исполнения всеми Работниками Организации, имеющими доступ к персональным данным.

1.5. Настоящая политика является общедоступной и размещается на официальных сайтах Организации.

1.6. Ознакомление Работников Организации с положениями настоящей Политики осуществляется под роспись.

2. Цели обработки персональных данных

2.1. Организация осуществляет обработку персональных данных в целях:

- предоставления субъектам персональных данных, не являющихся сотрудниками организации, информационных услуг;
- заключения с Субъектом персональных данных любых договоров и их дальнейшего исполнения;
- информирования клиентов о ходе исполнения оказываемых услуг;
- осуществления маркетинговых исследований и анализа их результатов, проведения акций, опросов, исследований;
- создание баз данных;
- предоставления Субъекту персональных данных информации об оказываемых Организацией услугах;
- ведения кадровой работы и организации учета Работников Организации;
- привлечение и отбор Кандидатов на работу в Организации;
- осуществления прохода посетителей на территорию Организации;
- осуществления Организацией Административно-хозяйственной деятельности;

3. Классификация персональных данных и Субъектов персональных данных

3.1. К персональным данным относится любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (Субъекту персональных данных), обрабатываемая Организацией для достижения заранее определенных целей.

3.2. Организация не осуществляет обработку специальных категорий персональных данных, касающихся расовой и национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни и судимости физических лиц.

3.3. Организация осуществляет обработку персональных данных следующих категорий Субъектов персональных данных:

- физические лица, являющиеся Кандидатами на работу;
- физические лица, являющиеся Работниками Организации;
- физические лица, осуществляющие выполнение работ по оказанию услуг и заключившие с Организацией договор гражданско-правового характера;
- физические лица, являющиеся пользователями сайтов Организации и услуг, предоставляемых на них;
- физические лица, не относящиеся к Клиентам Организации, заключившие или намеривающиеся заключить с Организацией договорные отношения в связи с осуществлением Организацией Административно-хозяйственной деятельности;
- физические лица, персональные данные которых сделаны ими общедоступными, а их обработка не нарушает их прав и соответствует требованиям, установленным Законодательством о персональных данных;
- иные физические лица, выразившие согласие на обработку Организацией их персональных данных.

4. Общие принципы обработки персональных данных

4.1. Организация осуществляет обработку персональных данных на основе общих принципов:

- законности заранее определенных конкретных целей и способов обработки персональных данных;
- обеспечения надлежащей защиты персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;
- соответствия объема, характера и способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- хранения персональных данных в форме, позволяющей определить Субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

- уничтожения или обезличивания персональных данных по достижении целей их обработки, если срок хранения персональных данных не установлен законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект персональных данных;

- обеспечения конфиденциальности и безопасности обрабатываемых персональных данных.

4.2. В рамках обработки персональных данных для Субъекта персональных данных и Организации определены следующие права:

4.2.1. Субъект персональных данных имеет право:

- получать информацию, касающуюся обработки его персональных данных, в порядке, форме и сроки, установленные Законодательством о персональных данных;

- требовать уточнения своих персональных данных, их Блокирования или Уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными, не являются необходимыми для заявленной цели обработки или используются в целях, не заявленных ранее при предоставлении Субъектом персональных данных согласия на обработку персональных данных;

- принимать предусмотренные законом меры по защите своих прав;

- отозвать свое согласие на обработку персональных данных.

4.2.2. Организация имеет право:

- обрабатывать персональные данные Субъекта персональных данных в соответствии с заявленной целью;

- требовать от Субъекта персональных данных предоставления достоверных персональных данных, необходимых для исполнения договора, оказания услуги, идентификации Субъекта персональных данных, а также в иных случаях, предусмотренных Законодательством о персональных данных;

- обрабатывать общедоступные персональные данные физических лиц;

- осуществлять обработку персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации;

- поручить обработку персональных данных другому лицу с согласия Субъекта персональных данных.

5. Основные участники процесса обработки персональных данных

5.1. В целях осуществления эффективного управления процессом обработки персональных данных определены основные его участники.

5.1.1. Генеральный директор Организации:

- определяет, рассматривает и утверждает политику Организации в отношении обработки персональных данных;

- назначает лицо, ответственное за организацию обработки персональных данных и определяет подразделение, ответственное за обеспечение безопасности персональных данных.

5.1.2. Лицо, ответственное за организацию обработки персональных данных:

- организует и контролирует разработку процесса обработки персональных данных (совершаемых с использованием средств автоматизации или без использования таких средств) в соответствии с требованиями Законодательства о персональных данных и настоящей Политики;

- осуществляет управление процессом обработки персональных данных;

- разрабатывает и представляет для утверждения Генеральному директору Организации политику и локальные документы, касающиеся вопросов обработки персональных данных;

- осуществляет анализ, оценку и прогноз риска, связанного с нарушением процедур обработки персональных данных в Организации, защиты персональных данных.

- осуществляет внутренний контроль за соблюдением Организации и ее работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

- доводит до сведения работников Организации положения законодательства Российской Федерации о персональных данных, локальные акты по вопросам обработки персональных данных, требования к защите персональных данных;

- организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.1.3. Подразделение по обеспечению безопасности:

- осуществляет разработку и организацию применения правовых, организационных и технических мер защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также иных неправомерных действий в отношении персональных данных;

- осуществляет определение угроз безопасности персональных данных при их обработке;

- осуществляет оценку, обеспечение и контроль уровня защищенности информационных систем персональных данных;

- осуществляет оценку эффективности принимаемых мер по обеспечению безопасности персональных данных;

- осуществляет взаимодействие с органами государственной власти по вопросам защиты персональных данных;

- осуществляет методологическую помощь работникам Организации по вопросам обработки и защиты персональных данных;

- разрабатывает внутренние процедуры, направленные на обеспечение безопасности и защиты персональных данных.

5.1.4. Юридический отдел:

- осуществляет мониторинг законодательства и доведение до сведения заинтересованных подразделений информации об изменении правовых норм;

- своевременно информирует лиц (-о), ответственных (-ого) за организацию обработки персональных данных об изменениях Законодательства о персональных данных;

- осуществляет представительство Организации в судебных, правоохранительных и иных правоприменительных органах по судебным, административным делам по вопросам обработки персональных данных в части защиты прав, законных интересов, деловой репутации Организации и ее должностных лиц.

6. Организация системы управления процессом обработки персональных данных

6.1. Обработка персональных данных Субъекта персональных данных осуществляется с его согласия на обработку персональных данных, а также без такового, если Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является Субъект персональных данных, а также для заключения договора по инициативе Субъекта персональных данных или договора, по которому Субъект персональных данных будет

являться выгодоприобретателем или поручителем или в иных случаях, предусмотренных Законодательством о персональных данных.

6.2. Организация вправе поручить обработку персональных данных другому лицу с согласия Субъекта персональных данных, если иное не предусмотрено федеральным законом. Такая Обработка персональных данных осуществляется только на основании договора, заключенного между Организацией и третьим лицом, в котором должны быть определены:

- перечень действий (операций) с персональными данными, которые будут совершаться третьим лицом, осуществляющим обработку персональных данных;
- цели обработки персональных данных;
- обязанности третьего лица соблюдать конфиденциальность персональных данных и обеспечивать их безопасность при обработке, а также требования к защите обрабатываемых персональных данных.

6.3. Организация осуществляет передачу персональных данных государственным органам в рамках их полномочий в соответствии с законодательством Российской Федерации.

6.4. Организация несет ответственность перед Субъектом персональных данных за действия лиц, которым она поручает обработку персональных данных Субъекта персональных данных.

6.5. Доступ к обрабатываемым персональным данным предоставляется только тем Работникам Организации, которым он необходим в связи с исполнением ими своих должностных обязанностей и с соблюдением принципов персональной ответственности.

6.6. Обработка персональных данных прекращается при достижении целей такой обработки, а также по истечении срока, предусмотренного законом, договором, или согласием Субъекта персональных данных на обработку его персональных данных. При отзыве Субъектом персональных данных согласия на обработку его персональных данных Обработка осуществляется только в пределах, необходимых для исполнения заключенных с ним договоров и в целях, предусмотренных законодательством Российской Федерации.

6.7. Обработка персональных данных осуществляется с соблюдением конфиденциальности, под которой понимается обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия Субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

6.8. Организация обеспечивает конфиденциальность персональных данных Субъекта персональных данных со своей стороны, со стороны своих аффилированных лиц, со стороны своих Работников, имеющих доступ к персональным данным физических лиц, а также обеспечивает использование персональных данных вышеуказанными лицами исключительно в целях, соответствующих закону, договору или иному соглашению, заключенному с Субъектом персональных данных.

7. Обеспечение безопасности персональных данных

7.1. Важнейшим обязательным условием реализации целей деятельности Организации является обеспечение необходимого и достаточного уровня защищенности, а также соблюдение конфиденциальности, целостности и доступности обрабатываемых персональных данных на всех этапах работы с ними.

7.2. Организация обеспечивает режим защиты персональных данных, соответствующий третьему уровню защищенности персональных данных.

7.3. Обеспечение безопасности обрабатываемых персональных данных осуществляется с применением комплексной системы организационно-технических и правовых мероприятий по защите информации, с учетом требований Законодательства о персональных данных, принятых в соответствии с ним нормативных правовых актов.

Система информационной безопасности Организации непрерывно развивается и совершенствуется на базе требований международных и национальных стандартов информационной безопасности, а также лучших мировых практик.

7.4. В целях организации и обеспечения безопасности персональных данных Организация обеспечивает следующие меры:

- назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;
- строгое ограничение круга лиц, имеющих доступ к персональным данным;
- ознакомление работников с требованиями федерального законодательства и нормативных документов Компании по обработке и защите персональных данных;
- обеспечение учёта и хранения материальных носителей персональных данных в условиях, обеспечивающих сохранность и недопущение несанкционированного доступа к ним;
- регулярная оценка и определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
- регистрация и учёт действий пользователей информационных систем персональных данных;
- применение средств разграничения и контроля доступа к информации, информационным ресурсам, информационным системам, коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;
- реализация парольной защиты при осуществлении доступа пользователей к информационной системе персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- применение средств межсетевое экранирования;
- осуществление антивирусного контроля, предотвращение внедрения вредоносных программ (программ-вирусов) и программных закладок;
- применение средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на машинных носителях информации;
- обнаружение вторжений;
- резервное копирование информации;
- обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- централизованное управление системой защиты персональных данных;
- обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.
- размещение технических средств обработки персональных данных, в пределах границ охраняемой территории;
- обеспечение пропускного режима на территорию Организации;

8. Заключительные положения

8.1. Организация, а также ее должностные лица и Работники несут гражданско- правовую, административную и иную ответственность за несоблюдение принципов и условий обработки персональных данных физических лиц, а также за разглашение или незаконное использование персональных данных в соответствии с законодательством Российской Федерации.

8.2. Политика является общедоступной и подлежит размещению на официальных сайтах Организации.