УТВЕРЖДЕНО

приказом генерального директора

ЗАО «ГК АККОРД»

№ 01 от «03 » февраля 2016г.

Политика в отношении обработки персональных данных
ЗАО «ГК АККОРД»

Москва
2016

1. Назначение

Настоящая Политика в отношении обработки персональных данных ЗАО «ГК АККОРД» (далее-Политика) разработана в соответствии с п. 2 ст. 18.1 Федерального закона РФ «О персональных данных» и действует в отношении всех персональных данных, обрабатываемых в ЗАО «ГК АККОРД» (далее- Компания).

Целью настоящей Политики является установление правил обработки персональных данных в Компании с учетом необходимости выполнения законодательства Российской Федерации о персональных данных и защиты интересов Компании, ее клиентов, партнеров и работников.

2. Общие положения

Действие Политики распространяется на все процессы Компании, в рамках которых осуществляется обработка персональных данных субъектов персональных данных (далее – ПДн) всех категорий, а также на подразделения, принимающие участие в указанных процессах.

Основные положения документа могут быть на основе договора (соглашения) распространены также на подразделения других организаций и учреждений, осуществляющие взаимодействие с Компанией в качестве поставщиков и потребителей (пользователей) информации.

3. Принципы обработки ПДн

Обработка ПДн в Компании осуществляется на основе следующих принципов:

- обработка ПДн осуществляется на законной и справедливой основе;
- ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн;
- не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместных между собой;
- обработке подлежат только ПДн, которые отвечают целям их обработки;
- содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки. Обрабатываемые ПДн не являются избыточными по отношению к заявленным целям обработки;
- при обработке ПДн обеспечивается точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки.
- хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению, либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Принципы обеспечения безопасности ПДн

Основной задачей обеспечения безопасности ПДн при их обработке в Компании является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

Для обеспечения безопасности ПДн Компания руководствуется следующими принципами:

1. законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

2. системность: обработка ПДн в Компании осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3. комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Компании (далее - ИС) и других имеющихся в Компании систем и средств защиты;

4. непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

5. своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

6. преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Компании с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

7. персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

8. минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для

выполнения их должностных обязанностей;

9. гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем ПДн Компании (далее - ИСПДн), а также объема и состава обрабатываемых ПДн;

10. открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн Компании не дают возможности преодоления имеющихся в Компании систем защиты возможными нарушителями безопасности ПДн;

11. научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

12. специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация систем защиты ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

13. эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Компании предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Компании до заключения договоров;

14. наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

15. непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

5. Условия обработки ПДн

Обработка ПДн осуществляется с соблюдением принципов и правил, установленных Федеральным законом «О персональных данных». Обработка ПДн допускается в следующих случаях:

- обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;
- обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- обработка ПДн осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания ПДн. Исключение составляет обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи;
- осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн, либо по его просьбе (далее - ПДн, сделанные общедоступными субъектом ПДн);
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

В случае необходимости Компания может включить ПДн субъектов в общедоступные источники ПДн, при этом Компания берет письменное согласие субъекта на обработку его ПДн.

Компания не осуществляет обработку специальных категорий ПДн.

Биометрические ПДн (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн) в Компании не обрабатываются.

Компания не осуществляет трансграничную передачу ПДн.

Принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, не осуществляется.

При отсутствии необходимости письменного согласия субъекта на обработку его ПДн согласие субъекта может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме.

Компания вправе поручить ПДн данных другому лицу с согласия субъекта ПДн, если иное не предусмотрено

федеральным законом, на основании заключаемого с этим лицом договора (далее - поручение оператора). При этом Компания в договоре обязует лицо, осуществляющее обработку ПДн по поручению Компании, соблюдать принципы и правила обработки ПДн, предусмотренные настоящим документом и Федеральным законом «О персональных данных».

В случае если Компания поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет Компания. Лицо, осуществляющее обработку ПДн по поручению Компании, несет ответственность перед Компанией.

Компания обязуется и обязует иные лица, получившие доступ к ПДн, не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

6. Права субъекта ПДн

В соответствии с Федеральным законом «О персональных данных» субъект ПДн имеет право:

Получить сведения касающиеся обработки ПДн оператором, а именно:

- подтверждение факта обработки ПДн оператором;
- правовые основания и цели обработки ПДн;
- цели и применяемые оператором способы обработки ПДн;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

Потребовать от оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Заявить возражение против принятия в отношении себя решений, порождающих юридические последствия на основе исключительно автоматизированной обработки ПДн.

Отозвать согласие на обработку ПДн в предусмотренных законом случаях.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами РФ.

7. Обязанности Компании

В соответствии с требованиями Федерального закона «О персональных данных» Компания обязана:

Предоставлять субъекту ПДн по его запросу информацию, касающуюся обработки его ПДн, либо на законных основаниях предоставить отказ.

По требованию субъекта ПДн уточнять обрабатываемые ПДн, блокировать или удалять, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Вести Журнал учета обращений субъектов ПДн, в котором должны фиксироваться запросы субъектов ПДн на получение ПДн, а также факты предоставления ПДн по этим запросам.

Уведомлять субъекта ПДн до начала обработки его ПДн в том случае, если ПДн были получены не от субъекта ПДн. Исключение составляют следующие случаи:

- Субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;
- ПДн получены Компанией на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
- Компания осуществляет обработку ПДн для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;
- Предоставление субъекту ПДн сведений, содержащихся в Уведомлении об обработке ПДн, нарушает права и законные интересы третьих лиц.

В случае достижения цели обработки ПДн незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Компанией и субъектом ПДн либо если Компания не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

В случае отзыва субъектом ПДн согласия на обработку своих ПДн прекратить обработку ПДн и уничтожить ПДн в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Компанией и субъектом ПДн. Об уничтожении ПДн Компания обязана уведомить субъекта ПДн.

В случае поступления требования субъекта о прекращении обработки ПДн в целях продвижения товаров, работ, услуг на рынке немедленно прекратить обработку ПДн.

8. Меры по обеспечению безопасности ПДн при их обработке

При обработке ПДн Компания принимает необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Обеспечение безопасности ПДн достигается, в частности:

- определением угроз безопасности ПДн при их обработке в ИСПДн;
- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- учетом машинных носителей ПДн;
- обнаружением фактов несанкционированного доступа к ПДн и принятием мер;
- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

9. Основные мероприятия по обеспечению безопасности ПДн

Мероприятия по защите ПДн реализуются в Компании в следующих направлениях:

1. предотвращение утечки информации, содержащей ПДн, по техническим каналам связи и иными способами;
2. предотвращение несанкционированного доступа к содержащей ПДн информации, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;
3. защита от вредоносных программ;
4. обеспечение безопасного межсетевого взаимодействия;
5. обеспечение безопасного доступа к сетям международного информационного обмена;
6. анализ защищенности ИСПДн;
7. обеспечение защиты информации с использованием шифровальных (криптографических) средств при передаче ПДн по каналам связи;
8. обнаружение вторжений и компьютерных атак;
9. осуществления контроля за реализацией системы защиты ПДн.

Мероприятия по обеспечению безопасности ПДн включают в себя:

1. реализацию разрешительной системы допуска пользователей (Работников) к информационным ресурсам ИС и связанным с их использованием работам, документам;
2. разграничение доступа пользователей ИСПДн и обслуживающих ИСПДн Работников к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
3. регистрацию действий пользователей и обслуживающих ИСПДн Работников, контроль несанкционированного доступа и действий пользователей и обслуживающих Работников, а также третьих лиц;
4. использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
5. предотвращение внедрения в ИС вредоносных программ и программных закладок, анализ принимаемой по информационно-телекоммуникационным сетям (сетям связи общего пользования) информации, в том числе на наличие

компьютерных вирусов;

6. ограничение доступа в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации, содержащие ПДн;

7. размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

8. организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку ПДн;

9. учет и хранение съемных носителей информации, и их обращение, исключающее хищение, подмену и уничтожение;

10. резервирование технических средств, дублирование массивов и носителей информации;

11. реализацию требований по безопасному межсетевому взаимодействию ИС;

12. использование защищенных каналов связи, защита информации при ее передаче по каналам связи;

13. межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры ИС;

14. обнаружение вторжений в ИС, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

15. периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на ИС;

16. активный аудит безопасности ИС на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;

17. анализ защищенности ИС с применением специализированных программных средств (сканеров безопасности);

18. централизованное управление системой защиты ПДн в ИС.

В целях организации работ по обеспечению информационной безопасности ПДн в Компании определяются структурные подразделения, на которые возлагаются задачи:

1. по классификации и аттестации ИСПДн;

2. организации разработки модели угроз для каждой ИСПДн;

3. организации разработки технического проекта системы защиты информации для каждой ИСПДн;

4. закупки, установки, эксплуатации и администрирования средств защиты информации;

5. организации разрешительной системы допуска к информации, содержащей ПДн и разработке внутренних регулятивных документов Компании по этому вопросу;

6. организации реагирования на события безопасности;

7. контроля состояния системы защиты информации и планирования соответствующих мероприятий.

С целью поддержания состояния защиты ПДн на надлежащем уровне в Компании осуществляется внутренний контроль за эффективностью системы защиты ПДн и соответствием порядка и условий обработки и защиты ПДн установленным требованиям.

Внутренний контроль включает:

1. мониторинг состояния технических и программных средств, входящих в состав системы защиты ПДн;

2. контроль соблюдения требований по обеспечению безопасности ПДн (требований нормативных правовых актов и внутренних регулятивных документов в области обработки и защиты ПДн, требований договоров).

В целях осуществления внутреннего контроля в Компании проводятся периодические проверки условий обработки ПДн. Такие проверки осуществляются ответственным за организацию обработки ПДн в Компании либо комиссией, образуемой Генеральным директором Компании.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывается Генеральному директору Компании.

10. Изменение политики

Компания имеет право вносить изменения в настоящую Политику.

При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте Компании, если иное не предусмотрено новой редакцией Политики.