Утверждаю
Генеральный директор
ОАО «РСП ТПК КГРЭС»
_____М.В. Езжев
«__»_____2013 г.

ПОЛИТИКА
ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ОАО «РСП ТПК КГРЭС»

. Волгореченск
2013

1. Общие положения.

1.1. Настоящее Положение определяет цели, задачи и основные мероприятия по обеспечению безопасности персональных данных в ОАО «РСП ТПК КГРЭС» (далее — Общество) от несанкционированного доступа, неправомерного их использования или утраты. Настоящий документ определяет набор требований, связанных с получением, учетом, обработкой, накоплением и хранением информации, относящейся к персональным данным, содержащимся в ОАО «РСП ТПК КГРЭС»

1.2. Положение разработано в соответствии с действующим законодательством Российской Федерации в области защиты персональных данных:

1.2.1. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".

1.2.2. Постановления Правительства Российской Федерации от 15.09. 2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

1.2.3. Постановления Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

1.2.4. Нормативные документы уполномоченных органов.

1.3. Положение является основой для разработки локальных нормативных актов Общества по обеспечению безопасности ПДн.

1.4. Настоящий документ обязателен для исполнения подразделениями и должностными лицами, участвующими в обработке персональных данных.

Под должностным лицом понимается работник ОАО РСП ТПК КГРЭС», постоянно, временно или по специальному полномочию осуществляющий в соответствии с должностной инструкцией, распорядительными и организационно-распорядительными документами Общества.

1.5. Настоящее положение распространяется на работников Общества, включая работающих по договору подряда, на работников сторонних организаций, взаимодействующих с Обществом на основании соответствующих нормативных, правовых и организационно-распорядительных документов, а также на физических лиц, находящихся в гражданско-правовых отношениях с Обществом.

1.6.Принципы и требования по организации работы с персональными данными распространяются на все возможные носители информации, такие как:

- бумажные носители;
- электронные носители;

и на все возможные форматы представления персональных данных, такие как:

- документы;
- файлы;
- почтовые сообщения;
- базы данных;
- записи базы данных;
- другие информационные массивы.

1.7..Общество оставляет за собой право вносить необходимые изменения в Политику при изменении действующего законодательства РФ и условий своей деятельности.

В дополнение к настоящей Политике, при необходимости, Общество вправе разрабатывать другие внутренние нормативные документы, регламентирующие отдельные процессы управления персональными данными.

1.8.Обеспечение безопасности персональных данных является одной из приоритетных задач Общества.

1.9.Действующая редакция настоящей политики является общедоступной и размещается в информационной сети Интернет на официальном сайте ОАО «РСП ТПК КГРЭС» www.tpk-kgres.ru.

2. Термины и принятые сокращения.

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

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации 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.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Персональные данные, сделанные общедоступными субъектом персональных данных - ПД, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. Доступ к персональным данным

3.1.Доступ к персональным данным субъекта могут получить работники Общества, только в рамках исполнения своих должностных обязанностей. Доступ иных лиц к персональным данным, обрабатываемым ОАО «РСП ТПК КГРЭС», может быть предоставлен исключительно в предусмотренных законом случаях.

32.Допуск работников Общества к обработке ПДн осуществляется на основании «Списка работников, допущенных к обработке персональных данных…», утверждаемого Генеральным директором ОАО «РСП ТПК КГРЭС» не реже 1 раза в год.

3.3.Документы на бумажных носителях, содержащие персональные данные субъектов, хранятся в личных делах (каждого субъекта отдельно). Личные дела хранятся в бумажном виде в папках и размещаются в сейфе.

3.4.Хранение и обработка персональных данных осуществляется в порядке, исключающем несанкционированный доступ к персональным данным, в том числе третьих лиц.

3.5.При увольнении сотрудника, имеющего доступ к персональным данным субъектов, документы и иные носители, содержащие персональные данные, передаются руководителю подразделения, в котором работал сотрудник, доступ сотрудника к ИСПДн отзывается.

4. Обработка персональных данных.

4.1. Получение ПДн.

4.1.1. Все ПДн следует получать от самого субъекта. Если ПДн субъекта можно получить только у третьей стороны, то Субъект должен быть уведомлен об этом или от него должно быть получено согласие.

341.2. Оператор должен сообщить Субъекту о целях, предполагаемых источниках и способах получения ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа Субъекта дать письменное согласие на их получение.

4.1.3. Документы, содержащие ПДн, создаются путем:

- копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);
- внесения сведений в учетные формы;
- получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

4.2. Обработка ПДн.

4.2.1. Обработка персональных данных осуществляется:

- С согласия субъекта персональных данных на обработку его персональных данных;
- В случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- В случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных).

4.2.2 Цели обработки персональных данных

- обработка персональных данных для целей кадрового делопроизводства;
- обеспечение выполнения условий трудового договора;
- выполнение требований закона о воинском учёте;
- создание условий для назначения трудовых пенсий в соответствии с результатами труда каждого застрахованного лица;
- создание условий для начисления заработной платы, оплаты листков нетрудоспособности, пособий и предоставления льгот, установленных законодательством;
- подготовка, переподготовка работников, повышение квалификации работников с высшим образованием, руководящих работников и специалистов по направлениям деятельности;
- выполнение требований законов и других нормативных правовых актов РФ;

4.2.3. Категории субъектов персональных данных:

- физические лица, состоящие в трудовых отношениях
- близкие родственники лиц, состоящих в трудовых взаимоотношениях с ОАО «РСП ТПК КГРЭС»
- Физические лица, состоящие в гражданско-правовых отношениях
- Собственники и пользователи жилых помещений МКД, находящихся в управлении
- Руководители и (или) уполномоченные юридических лиц (ИП, ЧП), состоящих в договорных отношениях
- Физические лица, состоящие в договорных отношениях (получение услуг)
- Физические лица – соискатели на вакантные должности
- Физические лица - потребители и их законные представители;
- Физические лица - практиканты/стажеры.

4.2.4. ПДн, обрабатываемые Обществом:

- Данные полученные при осуществлении трудовых отношений;
- Данные полученные для осуществления отбора кандидатов на работу;
- Данные полученные при осуществлении гражданско-правовых отношений.

Полный список ПДн представлен в Перечне , утвержденном Генеральным директором Общества.

4.2.5. Принципы обработки персональных данных

Цели обработки ПДн соответствуют целям, заявленным при сборе ПДн.

Объем, состав и способы обработки ПДн соответствуют целям обработки ПДн.

Не допускается обработка ПДн, избыточных по отношению к целям обработки ПДн.

- Цели обработки персональных данных описаны в «Перечне персональных данных, обрабатываемых в ООО КБ «Дружба»».

Не допускается объединение информационных массивов, созданных для несовместимых между собой целей обработки ПДн.

ПДн подлежат уничтожению по достижении целей их обработки.

Обработка в ИСПДн Банка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни производится при наличии согласия субъекта ПДн либо при разрешении такой обработки Федеральным законодательством.

4.2.6. Обработка персональных данных ведется:

- С использованием средств автоматизации с передачей по внутренней сети юридического лица; с передачей по сети Интернет;
- Без использования средств автоматизации.

4.3. Хранение ПДн.

4.3.1. ПДн Субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.3.2. ПДн, зафиксированные на бумажных носителях хранятся в запираемых шкафах.

4.3.3. ПДн Субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

4.3.4. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках) в ИСПДн.

4.3.5. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4.4. Уничтожение ПДн

4.4.1. Уничтожение документов (носителей), содержащих ПДн производится путем сожжения, дробления (измельчения). Для уничтожения бумажных документов допускается применение шредера.

4.4.2. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.4.3. Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

4.5. Передача ПДн.

4.5.1. Общество поручает обработку ПДн третьим лицам в следующих случаях:

- Субъект выразил свое согласие на такие действия;
- Передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

4.5.2. Перечень лиц, которым передаются ПДн.
Третьи лица, которым передаются ПДн:

- Пенсионный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Банки для начисления заработной платы (на основании договора);
- Органы исполнительной власти;
- Негосударственные пенсионные фонды:
- судебные органы;
- и другие взаимодействующие с Обществом лица.

Передача персональных данных взаимодействующим с Обществом лицам может производиться только в предусмотренных законодательством случаях и осуществляется в соответствии с законодательством РФ и международными договорами (соглашениями) РФ.

5. Защита персональных данных.

5.1. В соответствии с требованиями нормативных документов в Обществе создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

5.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПД.

5.5. Основными мерами защиты ПД, используемыми Обществом, являются:

5.5.1. Назначение лица ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением Обществоом и его работниками требований к защите ПД;

5.5.2. Определение актуальных угроз безопасности ПД при их обработке в ИСПД, и разработка мер и мероприятий по защите ПД;

5.5.3. Разработка локальных нормативных актов в отношении обработки персональных данных;

5.5.4. Установление правил доступа к ПД, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПД в ИСПД;

5.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их должностным обязанностями;

5.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

5.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

5.5.8. Сертифицированное программное средство защиты информации от несанкционированного доступа;

5.5.9. Сертифицированные межсетевой экран и средство обнаружения вторжения;

4.5.10. Соблюдаются условия, обеспечивающие сохранность ПД и исключающие несанкционированный к ним доступ;

5.5.11. Обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;

5.5.12. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.5.13. Обучение работников Общества, непосредственно осуществляющих обработку персональных данных, в рамках требований законодательства Российской Федерации в части защиты персональных данных, в том числе документам, определяющими политику Общества в отношении обработки персональных данных, локальным нормативным актам по вопросам обработки персональных данных;

5.5.14. Осуществление внутреннего контроля и аудита.

6. Основные права субъекта ПД и обязанности оператора.

6.1. Основные права субъекта ПД:

6.1.1 Субъект персональных данных имеет право требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.1.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

6.1.3 Обращения к оператору и направлению ему запросов;

6.1.4 Обжалование действий или бездействия оператора.

6.2. Обязанности Оператора:

Оператор обязан:

- При сборе персональных данных предоставить субъекту персональных данных по его просьбе информацию о полученных ПДн
- в случаях если ПДн были получены не от субъекта ПДн, уведомить субъекта персональных данных;
- в случае отказа субъекта ПДн в предоставлении ПДн субъекту разъясняются юридические последствия такого отказа;

- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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;
- давать ответы на запросы и обращения Субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.

6.3 Условия обработки персональных данных

Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных ФЗ-152 «О персональных данных». Обработка персональных данных допускается в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных 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 персональных данных 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 персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;
- 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;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных 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 персональных данных;
- обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в ст. 15 ФЗ-152 «О

персональных данных», при условии обязательного обезличивания персональных данных;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

7. Уничтожение персональных данных

В случае достижения цели обработки Общество прекращает обработку ПДн, если иное не предусмотрено соглашением между Обществом и субъектом персональных данных.

В случае отзыва субъектом ПДн согласия на обработку своих ПДн Общество прекращает их обработку, если иное не предусмотрено соглашением между Обществом и субъектом ПДн, либо если Общество вправе осуществлять обработку ПДн без согласия субъекта ПД на основаниях, предусмотренных законом «О персональных данных» или другими федеральными законами.

В случае выявления неправомерной обработки ПДн Банк предпринимает меры по уничтожению этих ПДн в срок, не превышающий десяти рабочих дней со дня выявления неправомерной обработки ПДн.

В случае отсутствия возможности уничтожения ПДн в течение указанного срока, Общество осуществляет блокирование таких ПДн и обеспечивает уничтожение ПДн в срок, не превышающий 6 месяцев со дня выявления неправомерной обработки ПДн, если иной срок не установлен федеральным законодательством.

В случае если уничтожение ПДн было произведено по результатам обработки обращения субъекта ПДн и (или) запроса уполномоченного органа по защите прав субъектов ПДн, о предпринятых действиях Общество уведомляет субъекта ПДн и (или) уполномоченный орган по защите прав субъектов ПД.

ПДн на бумажных носителях уничтожаются с помощью средств, гарантирующих невозможность восстановления носителя или посредством вычеркивания (вымарывания и т.п.) ПДн.

Уничтожение информации с машиночитаемых носителей ПДн, пришедших в негодность или утративших практическую ценность, производится способом, исключающим возможность использования и восстановления информации.

8. Защита персональных данных

В соответствии со статьей 18.1 ФЗ-152 от 27.07.2006г. «О персональных данных» Общество самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения требований законодательства. Общество принимает следующие меры:

- издает документы, определяющие политику в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- назначает ответственного за организацию обработки ПДн;
- применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных;
- осуществляет внутренний контроль и аудит соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Общества в отношении обработки персональных данных, локальным актам Банка;
- доводит до сведения работников Общества, непосредственно осуществляющих обработку персональных данных, положения законодательства Российской Федерации о персональных данных, в том числе требования к защите персональных данных, документы, определяющие политику Общества в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, и проводит обучение указанных работников.

9. Уведомление уполномоченного органа по защите прав субъектов ПДн

В случаях, установленных Федеральным законом «О персональных данных», Общество направляет уведомление в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор).

В случае изменения сведений, указанных в уведомлении, а также в случае прекращения обработки персональных данных Общество уведомляет об этом Роскомнадзор в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом.

Уведомление должно содержать следующие сведения:

- наименование (фамилия, имя, отчество), адрес оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- фамилия, имя, отчество физического лица, ответственного за организацию обработки персональных данных, и номера его контактных телефонов, почтовый адрес и адрес электронной почты;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ.

10. Внутренний контроль

Внутренний контроль при обработке персональных данных направлен на обеспечение требований действующего законодательства Российской Федерации в сфере обработки персональных данных, внутренних нормативных документов Общества.

В случае выявления недостатков в осуществлении сотрудниками обработки персональных данных, обнаруженные недостатки документально фиксируются и предоставляются на рассмотрение Генеральному директору Общества.