**Сведения**

**о реализуемых требованиях к защите персональных данных**

Для защиты персональных данных работников, клиентов и контрагентов в ООО МКК «ГлавКредит-Урал» приняты правовые, организационные и технические меры:

1. **Правовые меры:**
   1. Разработаны и введены в действие локальные акты по вопросам обработки и защиты персональных данных работников, клиентов и контрагентов ООО МКК «ГлавКредит-Урал»:

* Политика в отношении обработки и защиты персональных данных.
* Положение о защите персональных данных работников, клиентов и контрагентов ООО МКК «ГлавКредит-Урал».
* Положение о порядке обезличивания персональных данных и работы с обезличенными персональными данными ООО МКК «ГлавКредит-Урал».
* Положение об антивирусной защите при обработке персональных данных и иной конфиденциальной информации ООО МКК «ГлавКредит-Урал».
* Положение о парольной защите при обработке персональных данных и иной конфиденциальной информации ООО МКК «ГлавКредит-Урал».
* Положение об ответственности работников ООО МКК «ГлавКредит-Урал» за разглашение персональных данных и несанкционированный доступ к персональным данным.
  1. Отказ от любых способов обработки персональных данных, не соответствующих требованиям законодательства Российской Федерации о персональных данных.

1. **Организационные меры.**
   1. Приказом ООО МКК «ГлавКредит-Урал» назначен ответственный за обеспечение информационной безопасности, за организацию обработки персональных данных, а также сбор, хранение, обработку и уничтожение персональных данных работников, клиентов и контрагентов ООО МКК «ГлавКредит-Урал», за разработку и осуществление мероприятий по обеспечению информационной безопасности и защиты персональных данных;
   2. Разработаны и введены в действие:

* Инструкция ответственного за организацию обработки персональных данных
* Инструкция пользователя по обеспечению безопасности обработки персональных данных при возникновении нештатных ситуаций в ООО МКК «ГлавКредит-Урал».
* Правила рассмотрения запросов субъектов персональных данных или их представителей в ООО МКК «ГлавКредит-Урал».
* Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных ООО МКК «ГлавКредит-Урал».
* Инструкция о порядке обработки персональных данных без использования средств автоматизации в ООО МКК «ГлавКредит-Урал».
* План мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных.
* Инструкция по проведению антивирусного контроля в информационной системе персональных данных.
* Инструкция пользователя по антивирусной защите.
  1. Организованы и осуществляются:
* Прием и обработка обращений и запросов субъектов персональных данных или их представителей;
* Контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
* Обработка персональных данных работников, клиентов и контрагентов ООО МКК «ГлавКредит-Урал», осуществляется с их письменного согласия.
  1. Определены:
* Угрозы безопасности персональных данных, актуальных для информационных систем персональных данных;
* Перечни лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
* Места хранения персональных данных (материальных носителей).
  1. Организовано ознакомление работников, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, требованиями к защите персональных данных, локальными актами по вопросам обработки и защиты персональных данных, ответственностью за нарушение норм, регулирующих обработку и защиту персональных данных.
  2. Организовано обучение работников в соответствии с Программой подготовки и обучения сотрудников по информационной безопасности и защите персональных данных.

1. **Технические меры.**
   1. Приняты меры по защите от несанкционированного доступа к персональным данным (идентификация и проверка подлинности пользователя при входе в информационную систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов).
   2. Для выявления вредоносного программного обеспечения в информационных системах применяется антивирусное программное обеспечение.
   3. Производится резервное копирование баз данных, содержащих персональные данные, для возможности их восстановления при модификации или уничтожения вследствие несанкционированного доступа к ним.
   4. Помещения оборудованы охранными системами.
   5. Обеспечено хранение информации на бумажных и (или) электронных носителях в сейфах, специально оборудованных хранилищах, специально оборудованных помещениях.