

## Политика обработки персональных данных Пользователей

Настоящая Политика обработки персональных данных пользователей (далее — Политика) действует в отношении всей информации, включая персональные данные Пользователя, которую ООО «КОМПАНИЯ ЮСИЭС» (далее – Оператор) может получить во время использования Программного обеспечения, владельцем которого является Оператор.

### 1. Термины и определения

<b>Оператор</b>	означает общество с ограниченной ответственностью «КОМПАНИЯ ЮСИЭС», ОГРН 5077746794186, адрес местонахождения: 115280, г. Москва, Ленинская слобода, д. 19, часть ком 21э, ком. 56-59, организующее и (или) осуществляющее обработку Персональных Данных самостоятельно или совместно с Партнерами, а также определяющие цели обработки Персональных Данных, состав Персональных Данных, подлежащих обработке, действия (операции), совершаемые с Персональными Данными.
<b>Персональные данные</b>	означает любую информацию, относящуюся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).
<b>Пользователь</b>	физическое лицо (субъект персональных данных) любым способом использующее функциональные возможности Программного обеспечения.
<b>Закон</b>	означает Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
<b>Программное обеспечение</b>	любое программное обеспечение (программы для ЭВМ, мобильные приложения и пр.), выпускаемые под товарным знаком «г_кеерет», а также любые иные программы для ЭВМ, компьютерные сервисы и Интернет-ресурсы, правообладателем которых является Оператор и находящиеся под управлением Оператора.
<b>Обработка Персональных данных</b>	означает 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.
<b>Партнер</b>	юридическое лицо или индивидуальный предприниматель, оказывающий совместно с Оператором услуги Пользователю в объеме функциональных возможностей Программного обеспечения.
<b>Группа ПАО Сбербанк</b>	ПАО «Сбербанк России» и юридические лица, являющиеся дочерними зависимыми обществами (ДЗО) ПАО Сбербанк. Перечень ДЗО ПАО Сбербанк указан на официальном сайте ПАО Сбербанк <a href="http://www.sberbank.ru">www.sberbank.ru</a>
<b>ДЕЛИВЕРИ КЛАБ</b>	ООО «ДЕЛИВЕРИ КЛАБ» (ОГРН 1097746360568 ИНН 7705891253, адрес местонахождения 125167, город Москва, Ленинградский проспект, дом 39 строение 80, этаж 7 пом\ 1-6,8,9)

## **2. Общие положения**

- 2.1. Настоящая Политика определяет правила и принципы обработки Персональных данных, а также содержит сведения о реализуемых Оператором мероприятиях в целях защиты Персональных данных.
- 2.2. Оператор не контролирует и не несет ответственность за информацию третьих лиц, размещенную на сайтах, на которые Пользователь может перейти по ссылкам, доступным в Программном обеспечении. На таких сайтах и ресурсах у Пользователя могут собираться или запрашиваться иные Персональные данные.
- 2.3. Настоящая Политика публикуется Оператором во исполнение норм действующего законодательства Российской Федерации, в том числе статьи 18.1 Закона, и подлежит не реже 1 (одного) раза в 3 (три) года или при изменении законодательства. Поддержание в актуальном состоянии Политики обеспечивает сотрудник отдела информационной безопасности.

## **3. Персональные данные Пользователя, которые собирает и обрабатывает Оператор**

- 3.1. Оператор собирает и обрабатывает следующие Персональные данные Пользователей:
  - фамилия, имя, отчество;
  - IP адрес;
  - e-mail;
  - дата рождения;
  - должность;
  - место работы;
  - номер телефона;
  - тип смартфона и его операционной системы;
  - город местонахождения;
  - тип устройства и вид операционной системы;
  - данные файлов cookie.

## **4. Цель обработки Персональных данных**

- 4.1. Оператор осуществляет обработку только тех Персональных данных, которые необходимы для использования Программного обеспечения или исполнения договоров (пользовательских соглашений) с Пользователем.
- 4.2. Обработка Персональных данных осуществляется в следующих целях:
  - создание учетных записей, предоставление доступа к учетным записям в Программном обеспечении;
  - осуществление связи с Пользователем для направления уведомлений, запросов и информации, относящейся к работе Программного обеспечения, выполнения соглашений с Пользователем, его запросов и заявок;
  - анализа и исследований в целях улучшения функционирования Программного обеспечения, в том числе его качества, удобства, а также – разработки новых сервисов и услуг в рамках Программного обеспечения;
  - персонализация рекламных предложений с учетом информации, доступной о Пользователе на основании полученных метрических данных (например, Яндекс.Метрика, Google Analytics и пр.);
  - осуществление оплаты товаров и услуг на Интернет-ресурсах Оператора;
  - оказание Пользователю услуг Партнерами Оператора;
  - обработка заявок Пользователя на бронирование столов в ресторанах, совершенные через Программное обеспечение.

## **5. Условия Обработки Персональных данных и передачи их третьим лицам**

- 5.1. Обработка Персональных данных Пользователей осуществляется в течение срока, необходимого для достижения целей, определенных настоящей Политикой, любым законным способом, в том числе в информационных системах Персональных данных с использованием средств автоматизации или без использования таких средств.
- 5.2. Обработка Персональных данных Пользователей допускается исключительно с согласия субъекта персональных данных в порядке и объеме, предусмотренном Законом и обусловленном целями Обработки Персональных данных.
- 5.3. Оператор вправе предоставлять Персональные данные Пользователя, в том числе поручать Обработку Персональных данных, на основании заключаемых с ними договоров следующим третьим лицам:
  - Партнерам, а также иным подрядчикам, поставщикам услуг и другим третьим сторонам, которые привлекаются Оператором для оказания комплекса работ, услуг и (или) иных действий в целях функционирования, улучшения и осуществления иных действий в отношении Программного обеспечения.
  - Партнерам, осуществляющим реализацию копий Программного обеспечения на основании заключенного с Оператором лицензионного соглашения.
  - ДЕЛИВЕРИ КЛАБ.
  - Группа ПАО Сбербанк.

## **6. Сведения о реализуемых требованиях к защите персональных данных**

- 6.1. Безопасность Персональных данных, обрабатываемых Оператором, обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований федерального законодательства в области защиты персональных данных, выявлением и предотвращением инцидентов, связанных с неправомерным доступом к персональным данным и неправомерных действий с ними.
- 6.2. Для целенаправленного создания неблагоприятных условий и труднопреодолимых препятствий для нарушителей, пытающихся осуществить несанкционированный доступ к персональным данным в целях их получения, модификации, блокирования, уничтожения, заражения вредоносным программным кодом и совершения иных несанкционированных действий, Оператором применяются следующие организационно-технические меры:
  - назначение должностных лиц, ответственных за организацию обработки и обеспечение безопасности персональных данных;
  - ограничение состава работников, обрабатывающих персональные данные и имеющих доступ к персональным данным при выполнении своих трудовых обязанностей, регламентация порядка предоставления такого доступа;
  - ознакомление работников с требованиями законодательства и внутренних нормативных документов Оператора по обработке и защите персональных данных;
  - обеспечение учёта и хранения материальных носителей персональных данных и установление порядка обращения с ними, направленного на предотвращение их хищения, подмены, несанкционированного копирования и уничтожения;
  - определение угроз безопасности персональным данным при их обработке, формирование на их основе частных моделей угроз и постоянное поддержание их актуальности;
  - разработка на основе модели угроз системы защиты персональных данных для соответствующего уровня защищенности персональных данных;
  - регулярная проверка готовности и эффективности используемых средств защиты информации;
  - реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
  - парольная защита доступа пользователей к информационной системе персональных данных;

- регистрация и учёт действий пользователей информационных систем персональных данных;
- применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;
- применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на машинных носителях информации;
- осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ и программных закладок;
- применение межсетевое экранирования;
- обнаружение вторжений в корпоративную сеть Оператора, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищённости информационных систем персональных данных Оператора с применением специализированных программных средств (сканеров безопасности);
- централизованное управление системой защиты персональных данных;
- резервное копирование информации;
- обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;
- учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, машинных носителей персональных данных;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям по безопасности;
- систематическое проведение мониторинга действий пользователей, проведение разбирательств по фактам нарушения требований безопасности персональных данных;
- размещение технических средств обработки персональных данных в пределах охраняемой территории;
- организация пропускного режима на территорию Оператора, охраны помещений и собственно технических средств обработки персональных данных;
- поддержание технических средств охраны, сигнализации помещений в состоянии постоянной готовности, ведение видеонаблюдения.

## **7. Заключительные положения**

- 7.1. Иные права и обязанности Оператора, связанные с обработкой им персональных данных, определяются Законом.
- 7.2. Должностные лица Оператора, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую и уголовную ответственность в порядке, установленном законодательством и внутренними нормативными документами Оператора.
- 7.3. Направить соответствующее обращение в рамках реализации прав Пользователя в отношении своих Персональных Данных или оставить свои комментарии и предложения относительно условий настоящей Политики можно посредством отправки сообщения на адрес электронной почты [info@foodplexgroup.ru](mailto:info@foodplexgroup.ru).