



Утверждено

Приказом № 743/25 от «15» сентября 2025 г.

**Политика
обработки и защиты
персональных данных
ООО «Unitel»**

Ташкент 2025 г.

Содержание

1. Общие положения
2. Термины и определения
3. Принципы обработки персональных данных
4. Правовые основания для обработки персональных данных
5. Условия, цели и особенности обработки персональных данных
6. Права субъектов персональных данных
7. Защита персональных данных
8. Принципы защиты персональных данных
9. Передача персональных данных третьим лицам
10. Трансграничная передача персональных данных
11. Хранение и уничтожение персональных данных
12. Уполномоченное подразделение
13. Обязанности и ответственность работников Компании
14. Заключительные положения

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика обработки и защиты персональных данных (далее – Политика) определяет порядок обработки и защиты персональных данных в ООО «Unitel» (далее – Компания).

1.2. Политика разработана в соответствии с законодательством Республики Узбекистан (далее – РУз) о персональных данных.

1.3. Компания является собственником и оператором баз персональных данных и обеспечивает их обработку в соответствии с требованиями законодательства, а также защиту от несанкционированного доступа и иных незаконных действий, связанных с персональными данными.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Персональные данные** – зафиксированная на электронном, бумажном и (или) ином материальном носителе информация, относящаяся к определенному физическому лицу или дающая возможность его идентификации.

2.2. **Обработка персональных данных** – это реализация одного или совокупности действий в отношении персональных данных:

- сбор;
- систематизация;
- хранение;
- изменение;
- дополнение;
- использование;
- предоставление;
- распространение;
- передача;
- обезличивание;
- уничтожение.

2.3. **Субъект персональных данных** – физическое лицо, к которому относятся персональные данные.

2.4. **Официальный веб-сайт** - интернет-ресурс Компании, предназначенный для размещения официальной информации, взаимодействия с Субъектами персональных данных, а также для публикации обязательной информации в соответствии с законодательством и внутренними нормативными документами Компании, расположенный по адресу – <https://beeline.uz>.

2.5. **Услуги** – совокупность услуг и цифровых решений, предоставляемых Компанией и (или) Бизнес-партнёром, включая услуги связи, Цифровые сервисы, а также иные формы взаимодействия с Абонентами, Пользователями цифровых сервисов, Бизнес-партнёрами и иными лицами в рамках основной деятельности Компании.

2.6. **Цифровой сервис** - совокупность технологических решений, предоставляемых Компанией и (или) Бизнес-партнёром с использованием информационно-коммуникационных технологий (включая мобильные приложения, веб-платформы и иные системы), предназначенных для предоставления услуг пользователям.

2.7. **Абонент** – физическое лицо, с которым заключён договор на предоставление услуг связи, либо лиц, фактически использующий услуги связи Компании на основании такого договора (в том числе при регистрации на имя третьего лица).

2.8. Пользователь цифровых сервисов – физическое лицо, использующее Цифровые сервисы Компании и (или) Бизнес-партнёров на основании соответствующих пользовательских соглашений /оферт, независимо от наличия договора об оказании услуг связи.

2.9. Исполнитель (физическое лицо) — физическое лицо, с которым Компания взаимодействует на основании гражданско-правового договора (включая, но не ограничиваясь: договоры подряда, оказания услуг, авторские договоры), а также индивидуальный предприниматель, осуществляющий деятельность без образования юридического лица.

2.10. Бизнес-партнёр — юридическое или физическое лицо (включая индивидуальных предпринимателей), участвующее совместно с Компанией в реализации сервисов, продуктов, маркетинговых и бонусных программ, а также иных проектов на договорной основе.

2.11. Уполномоченный представитель – физическое лицо, действующее от имени или в интересах Бизнес-партнёра (юридического лица или индивидуального предпринимателя), включая потенциальных Бизнес-партнёров, на основании закона, устава, доверенности или иного правового основания, а также физические лица, персональные данные которых обрабатываются Компанией в связи с их статусом участника юридического лица (в том числе учредители, руководители, подписанты), независимо от факта заключения договора.

2.12. Третье лицо – любое лицо, не являющееся субъектом, собственником и (или) оператором, но связанное с ними обстоятельствами или отношениями по обработке персональных данных.

2.13. Трансграничная передача персональных данных – передача персональных данных за пределы территории РУз.

2.14. Обезличенные персональные данные – персональные данные, в отношении которых осуществлены действия, в результате которых определение их принадлежности конкретному субъекту персональных данных становится невозможным.

2.15. Агрегированные данные – обобщённые статистические сведения, сформированные на основе обезличенных персональных данных, не позволяющие идентифицировать конкретного субъекта, и отражающие совокупные характеристики (например, средние значения, количество, процент, распределение).

2.16. Автоматизированная обработка персональных данных - обработка персональных данных с использованием информационных технологий, программных средств, алгоритмов и автоматических систем, при которой действия с персональными данными осуществляются полностью или преимущественно без участия человека.

2.17. Уполномоченное подразделение – структурное подразделение Компании, создаваемое для обеспечения обработки и защиты персональных данных в соответствии с законодательством РУз о персональных данных.

2.18. Защита персональных данных – совокупность правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности и доступности персональных данных, а также на предотвращение их утраты, неправомерного доступа, изменения, уничтожения, распространения и иных противоправных действий.

2.19. Конфиденциальность персональных данных – состояние персональных данных, при котором обеспечена безопасность от их незаконной обработки.

2.20. Целостность персональных данных – состояние персональных данных, при котором они сохраняются в первоначальном и/или установленном виде, защищены от несанкционированного или случайного изменения, удаления или искажения, могут быть восстановлены в случае сбоя, утраты или повреждения.

2.21. Техническая информация – совокупность сведений, автоматически собираемых и обрабатываемых при использовании Субъектом персональных данных Услуг Компании, включая, но не ограничиваясь: идентификаторами устройств и модулей (IMEI, IMSI, MAC-адрес, серийный номер, модель, тип оборудования); сведениями о SIM-карте и подключении к базовым станциям (ID БС, регистрация, зона покрытия); IP-адресом, сетевыми параметрами, типом подключения, скоростью соединения, режимом роуминга; информацией об операционной системе и программном обеспечении (версия, идентификаторы, параметры использования); геоданными (страна, город, координаты, точка входа); системными журналами и логами (ошибки, события, обращения к API, сессии); cookie-файлами и аналогичными технологиями; сведениями об обращениях в техническую поддержку (дата, содержание, результат); иными автоматически формируемыми техническими данными, необходимыми для предоставления, поддержки, функционирования, анализа и обеспечения безопасности Услуг.

2.22. Поведенческий профиль – совокупность сведений, формируемых в процессе использования Субъектом персональных данных Услуг Компании, характеризующих его действия, предпочтения и уровень активности, включая действия на веб-сайтах и в мобильных приложениях (клики, переходы, длительность сессий, частота использования); автоматизированно сформированные поведенческие модели и характеристики (например, интересы, предпочтения, склонности, уровень вовлечённости); объёмы потребления, история использования Услуг, сценарии взаимодействия; аналитические выводы, полученные на основании алгоритмов Big Data и машинного обучения; иные сведения, отражающие индивидуальные особенности поведения Субъекта при использовании Услуг.

2.23. Финансовая информация – совокупность Персональных данных, отражающих финансовую активность Субъекта персональных данных при использовании Услуг Компании или взаимодействии с ней, включая, но не ограничиваясь: сведения о балансе, тарифах, начислениях, списаниях и задолженности; история платежей, в том числе дата, сумма, способ и назначение операций; информация о платёжных инструментах, используемых Субъектом (включая тип карты, платёжную систему, маскированный номер, токенизированные данные); сведения о транзакциях, совершённых в Цифровых сервисах Компании (в т.ч. покупках, подписках, бонусах и скидках); банковские и расчётные реквизиты, предоставленные для выплат или возвратов; иные сведения, прямо или косвенно отражающие операции Субъекта, хранящиеся или обрабатываемые в информационных системах Компании.

3. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных в Компании осуществляется в строгом соответствии с принципами, установленными законодательством РУз. Указанные принципы являются обязательными для соблюдения всеми работниками и Третьими лицами, участвующими в Обработке персональных данных, и служат основой для оценки законности обработки.

3.2. Нарушение любого из принципов Обработки персональных данных рассматривается как нарушение законодательства РУз и влечёт меры ответственности в соответствии с установленным порядком.

3.3. К основным принципам Обработки персональных данных относятся:

- 3.3.1. соблюдение конституционных прав и свобод человека и гражданина;
- 3.3.2. законность целей и способов Обработки персональных данных;
- 3.3.3. точность и достоверность Персональных данных;
- 3.3.4. конфиденциальность и защищенность Персональных данных;
- 3.3.5. равенство прав субъектов, собственников и операторов персональных данных;
- 3.3.6. безопасность личности, общества и государства;
- 3.3.7. прозрачность Обработки персональных данных;
- 3.3.8. минимизация объёма обрабатываемых Персональных данных;
- 3.3.9. соблюдение сроков хранения Персональных данных.

4. ПРАВОВЫЕ ОСНОВАНИЯ ДЛЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Компания осуществляет Обработку персональных данных при наличии одного из следующих правовых оснований, предусмотренных законодательством РУз:

- 4.1.1. на основании явного и добровольного согласия субъекта, которое предоставляется для конкретных целей обработки данных;
- 4.1.2. когда обработка необходима для выполнения договора, стороной которого является Субъект персональных данных, или для принятия мер по запросу субъекта данных до заключения такого договора;
- 4.1.3. если обработка требуется для исполнения обязательств, возложенных на Компанию, определенных законодательством;
- 4.1.4. если обработка необходима для защиты законных интересов Субъекта персональных данных или другого лица;
- 4.1.5. если обработка необходима для осуществления прав и законных интересов Компании или Третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и законные интересы Субъектов персональных данных;
- 4.1.6. в статистических или иных исследовательских целях при условии обязательного Обезличивания персональных данных;
- 4.1.7. если эти данные были получены из общедоступных источников, и их обработка не нарушает права и свободы Субъектов персональных данных.

5. УСЛОВИЯ, ЦЕЛИ И ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В целях соблюдения требований законодательства РУз о Персональных данных в Приложении к настоящей Политике определены категории Субъектов персональных данных, цели Обработки персональных данных, а также перечень обрабатываемых Персональных данных для каждой категории.

5.2. Компания осуществляет как Автоматизированную, так и неавтоматизированную Обработку персональных данных в объёме, необходимом для достижения целей, предусмотренных в настоящей Политике.

Компания не принимает решений, основанных исключительно на Автоматизированной обработке персональных данных, если такие решения порождают

юридические последствия для Субъекта персональных данных или иным образом затрагивают его права и законные интересы.

5.3. Компания вправе обрабатывать данные о действиях, предпочтениях и взаимодействии Субъектов персональных данных с Услугами (включая Поведенческий профиль, Технические и Финансовые данные) в целях предоставления, оптимизации и развития Услуг, при соблюдении принципов минимизации и недопустимости нарушения прав субъектов.

Обработка осуществляется автоматизированными средствами и не предусматривает индивидуализированной Обработки персональных данных со стороны работников Компании.

Результаты такой обработки формируются в агрегированном либо обезличенном виде, исключающем возможность идентификации конкретных субъектов.

Передача таких данных Партнёрам допускается исключительно в агрегированном и (или) обезличенном виде.

5.4. Согласие Субъекта персональных данных на Обработку персональных данных может предоставляться в следующих формах:

5.4.1. путём акцепта оферты (публичного договора), в которой прямо указаны цели Обработки персональных данных, в этом случае согласие считается предоставленным с момента принятия оферты;

5.4.2. путём подтверждения согласия с условиями предоставления услуг в Цифровых сервисах Компании;

5.4.3. путём заключения договора;

5.4.4. в виде отдельного документа, оформленного в письменной или электронной форме;

5.4.5. путём совершения конклюдентных действий, включая фактическое пользование услугами Компании;

5.4.6. иными способами, не противоречащими законодательству РУз.

5.5. В случаях, когда Обработка персональных данных осуществляется без согласия субъекта (например, для исполнения договора, на основании требований законодательства или для защиты прав и законных интересов Компании), Компания действует строго в рамках, установленных законодательством РУз.

5.6. В целях обеспечения безопасности, защиты имущества и предотвращения инцидентов на территории и объектах Компании осуществляется видеонаблюдение.

Данные, полученные с помощью видеонаблюдения, не обрабатываются Компанией с целью идентификации конкретных Субъектов персональных данных.

При этом передача записей видеонаблюдения может осуществляться в случаях, предусмотренных законодательством Республики Узбекистан, в том числе по запросу правоохранительных органов, судов или иных уполномоченных государственных органов.

5.7. В целях обеспечения пропускного режима и контроля доступа на территорию и объекты Компании, допускается обработка биометрических персональных данных работников, стажёров, практикантов, Исполнителей (физических лиц) и Уполномоченных представителей. Такая обработка осуществляется на основании согласия субъекта в соответствии с целями, определёнными в настоящей Политике, с соблюдением требований законодательства РУз о Персональных данных.

6. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Субъекты персональных данных обладают правами, предусмотренными законодательством РУз, включая право на доступ, исправление, ограничение,

уничтожение Персональных данных, а также иные права, направленные на защиту их законных интересов.

6.2. Запросы, связанные с реализацией прав Субъектов персональных данных, могут направляться следующими способами:

- по электронной почте на адреса, указанные на официальных ресурсах Компании;
- почтовым отправлением на юридический адрес Компании;
- лично при посещении офиса Компании.

6.3. Отзыв согласия на Обработку персональных данных, требование об уничтожении или приостановке Обработки персональных данных, необходимых для предоставления Услуг Компании, влечет за собой невозможность дальнейшего предоставления таких Услуг Компанией.

7. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Компания обеспечивает Защиту персональных данных в процессе их обработки в соответствии с требованиями законодательства РУз.

7.2. Защита персональных данных осуществляется посредством комплекса правовых, организационных, технических и иных мер, направленных на предотвращение несанкционированного доступа, утраты, изменения, раскрытия или уничтожения Персональных данных.

8. ПРИНЦИПЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Защита персональных данных в Компании осуществляется в строгом соответствии с принципами, установленными настоящей Политикой. Указанные принципы являются обязательными для соблюдения всеми работниками, участвующими в Обработке персональных данных, и служат основой для оценки защищенности.

8.2. Нарушение любого из принципов Обработки персональных данных рассматривается как нарушение Политики и влечёт меры ответственности в соответствии с установленным порядком.

8.3. Компания обеспечивает Защиту персональных данных, руководствуясь следующими принципами, вытекающими из требований законодательства РУз и международной практики информационной безопасности:

8.3.1. соблюдение установленного законодательством режима, исключающего несанкционированное раскрытие или распространение Персональных данных, без согласия субъекта либо при отсутствии иного правового основания;

8.3.2. целостность и сохранность – соблюдение требований и принятие мер для предотвращения утраты, искажения или несанкционированного изменения Персональных данных; Персональные данные должны сохраняться в актуальном, непротиворечивом и защищённом состоянии;

8.3.3. ограничение доступа – доступ к Персональным данным предоставляется строго ограниченному кругу лиц в пределах их должностных обязанностей, на основе принципов ролевого доступа и минимально необходимого объёма;

8.3.4. прозрачность и подотчётность – механизмы Защиты персональных данных подлежат документированию, а действия, связанные с обработкой и защитой данных, могут быть проверены и подтверждены;

8.3.5. закрепление ответственности – обеспечение закрепления обязанностей и ответственности за Защиту персональных данных в должностных инструкциях, соглашениях о конфиденциальности и иных внутренних нормативных документах,

регулирующих деятельность работников и иных лиц, допущенных к Обработке персональных данных.

9. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ

9.1. Передача Персональных данных Бизнес-партнёрам или Третьим лицам, включая трансграничную, допускается исключительно в рамках целей их обработки и при наличии правовых оснований, предусмотренных пунктами 4.1. и 10.2 настоящей Политики.

9.2. Должны быть соблюдены следующие меры безопасности:

- заключение договора с Бизнес-партнёром или Третьим лицом, содержащего обязательства по Защите персональных данных;
- оценка правомерности передачи и ведение реестра таких операций.

9.3. В случае, если взаимоотношения с Бизнес-партнёром или Третьим лицом предусматривают доступ к персональным данным, их обработку или передачу, в обязательном порядке должны быть зафиксированы положения о защите персональных данных. Эти положения могут быть оформлены непосредственно в тексте договора либо в виде отдельного соглашения о конфиденциальности (NDA) или иного дополнительного соглашения к договору.

10. ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Трансграничная передача персональных данных осуществляется только в том случае, если страна-получатель обеспечивает адекватную защиту прав Субъектов персональных данных.

10.2 Трансграничная передача персональных данных в страну, не обеспечивающую адекватную защиту прав Субъектов персональных данных, может осуществляться в следующих случаях:

- наличие согласия Субъекта персональных данных на Трансграничную передачу персональных данных;
- необходимость защиты конституционного строя РУз, охраны общественного порядка, прав и свобод граждан, здоровья и нравственности населения;
- предусмотренных международными договорами РУз.

11. ХРАНЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Персональные данные хранятся в форме, позволяющей определить Субъекта персональных данных, не дольше, чем этого требуют цели их обработки и установленные сроки хранения.

11.2. Если иное не предусмотрено законодательством РУз, Персональные данные хранятся в течение срока, необходимого для достижения целей обработки, но не более чем в течение общего срока исковой давности, установленного законодательством РУз, с момента прекращения договорных или иных правоотношений с Субъектом персональных данных.

11.3. По истечении сроков хранения Персональные данные подлежат уничтожению или обезличиванию, если иное не предусмотрено законодательством.

12. УПОЛНОМОЧЕННОЕ ПОДРАЗДЕЛЕНИЕ

12.1. В Компании создается Уполномоченное подразделение, в задачи которого входит организация Обработки и Защиты персональных данных.

12.2. Организация деятельности, задачи, права и обязанности Уполномоченного подразделения устанавливаются законодательством РУз, положением об Уполномоченном подразделении и иными внутренними нормативными документами Компании.

13. ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ КОМПАНИИ

13.1. Работники обязаны соблюдать нормы законодательства РУз и внутренних нормативных документов Компании о Персональных данных.

13.2. Работники обязаны оказывать содействие Уполномоченному подразделению в осуществлении контроля за соблюдением законодательства РУз и внутренних нормативных документов Компании о Персональных данных.

13.3. При приеме на работу работник должен подписать обязательство неразглашении конфиденциальной информации и Персональных данных и ознакомиться с настоящей Политикой.

13.4. Работники Компании несут персональную ответственность за нарушение норм законодательства РУз, настоящей Политики и иных внутренних нормативных документов Компании о Персональных данных.

13.5. Работники Компании, непосредственно осуществлявшие работу с Персональными данными, в случае перевода на другую должность, смены позиции внутри Компании либо увольнения обязаны в установленном порядке передать все материальные носители информации (включая бумажные документы и иные носители, содержащие Персональные данные). Технические средства, предоставленные Компанией (в том числе ноутбуки, стационарные компьютеры и иные устройства), подлежат возврату и, при служебной необходимости, могут быть проверены на предмет выявления неправомерных действий.

14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

14.1. Настоящая Политика является внутренним нормативным документом Компании и обязательна для исполнения всеми работниками, а также иными лицами, вовлечёнными в процессы Обработки персональных данных.

14.2. Политика размещается в открытом доступе на Официальном веб-сайте и в Цифровых сервисах Компании в разделе, доступном для всех пользователей.

14.3. Политика вступает в силу с момента её размещения в указанных источниках, если иное не предусмотрено самой Политикой или отдельным решением Компании.

14.4. Компания вправе вносить изменения в Политику без специального уведомления Субъектов персональных данных. Новая редакция считается действующей с момента её размещения на Официальном веб-сайте и в Цифровых сервисах Компании, если иное не предусмотрено в новой редакции.

Приложение

**КАТЕГОРИИ
СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ,
ЦЕЛИ ОБРАБОТКИ И ПЕРЕЧЕНЬ ОБРАБАТЫВАЕМЫХ
ПЕРСОНАЛЬНЫХ ДАННЫХ**

Настоящим Приложением определяются категории Субъектов персональных данных, цели обработки и перечень обрабатываемых персональных данных в Компании. Оно применяется в отношении всех процессов Обработки персональных данных, осуществляемых Компанией, включая Автоматизированную и неавтоматизированную обработку.

Субъекты персональных данных	Цели обработки персональных данных	Перечень персональных данных
Абоненты Компании	1. Оказание и сопровождение Услуг - предоставление Услуг Компании, включая заключение и исполнение договоров, регистрацию и авторизацию в цифровых системах, предоставление услуг связи и доступа к Услугам Компании и Бизнес-партнёров; сопровождение оказания Услуг, включая ведение расчётов и биллинга, выставление счетов, учёт платежей, управление задолженностью и оформление платёжных операций. 2. Идентификация, безопасность и правовая защита: – идентификация и аутентификация Абонентов, в том числе при использовании мобильных приложений, личных кабинетов, через номера телефонов, идентификаторы устройств и иные механизмы установления личности; обеспечение безопасности доступа к информационным системам и приложениям, защита от мошенничества и несанкционированного доступа, выявление, предотвращение и расследование подозрительных действий; – реализация прав и законных интересов Компании, включая защиту интересов в рамках досудебных и судебных процессов, а также взаимодействие с государственными органами в соответствии с законодательством и по официальным запросам.	– фамилия, имя, отчество; – дата и место рождения; – реквизиты документа, удостоверяющего личность; – ПИНФЛ; – пол; – гражданство; – номер телефона; – адрес электронной почты; – адрес регистрации по месту жительства; – информация об оказываемых услугах связи (в том числе информация о договоре об оказании услуг связи, информация, содержащаяся в иных документах, формируемых в период оказания услуг связи); – детализация расходов по номеру телефона; – Техническая информация; – Поведенческий профиль; – Финансовая информация.

3. Работа с клиентским опытом и качеством обслуживания - повышение качества предоставляемых Услуг, включая обработку обращений и жалоб, техническую поддержку, устранение сбоев, проведение опросов удовлетворённости, анализ обратной связи; предоставление персонализированного интерфейса и сервисов в цифровой среде.

4. Информационные коммуникации и уведомления - информирование Абонентов о новых продуктах, услугах, тарифах, изменениях условий обслуживания, акциях, обновлениях приложений и иной информации, связанной с обслуживанием.

5. Маркетинг и коммерческое взаимодействие:

- предоставление услуг триггерной и таргетированной коммуникации, включая SMS-рассылки, автоматизированные IVR-звонки, коммерческие предложения и иную информацию, формируемую на основании действий Абонента, его истории обслуживания, поведения в Цифровых сервисах, событий и предпочтений;

- реализация маркетинговых мероприятий, направленных на повышение вовлечённости и лояльности Абонентов, формирование персонализированных предложений, участие в акциях, бонусных и партнёрских программах, направление рекламной и информационной коммуникации.

6. Аналитика, прогнозирование и взаимодействие с Бизнес-партнёрами:

- реализация проектов по анализу пользовательского поведения, предпочтений и потребительских трендов, включая сбор и анализ поведенческих данных, логов навигации, пользовательских сценариев и параметров взаимодействия с Цифровыми сервисами, моделирование поведения и прогнозирование спроса с использованием технологий Big Data и машинного обучения, а также оптимизацию Услуг Компании;

- применение алгоритмов скоринга, включая оценку платёжной дисциплины,

	анализ рисков, прогнозирование вероятности отклика на предложения на основе данных об активности, предпочтениях и истории взаимодействия с Услугами; – в рамках указанных целей допускается передача Обезличенных персональных данных и (или) Агрегированных данных, для оказания услуг Бизнес-партнёрам, при условии невозможности идентификации Субъектов персональных данных. 7. Передача данных Бизнес-партнёрам и Третьим лицам в рамках исполнения договорных обязательств, оказания Услуг, предоставления функциональности, интеграции или взаимодействия с Цифровыми сервисами и продуктами Бизнес-партнёров.	
Пользователи цифровых сервисов	1. Предоставление и сопровождение Цифровых сервисов - предоставление Цифровых сервисов Компании и Бизнес-партнёров, включая регистрацию и сопровождение учётной записи пользователя, создание личного кабинета в мобильных приложениях и на веб-сайтах, привязку аккаунта к номеру телефона или другим идентификаторам, восстановление доступа, управление настройками профиля и Персональными данными. 2. Обеспечение безопасности и стабильной работы - обеспечение безопасности и бесперебойной работы Цифровых сервисов, включая защиту от несанкционированного доступа, утечки данных и мошенничества, контроль корректности авторизации, ведение технических логов и мониторинг работоспособности мобильных приложений и веб-сайтов. 3. Анализ пользовательского поведения и технической аналитики - сбор и обработка данных о действиях пользователей (клики, навигация, просмотры и иные сценарии взаимодействия) в целях анализа поведения, определения предпочтений, выявления затруднений в интерфейсе и оценки эффективности функций мобильных	– фамилия, имя, отчество; – дата и место рождения; – номер телефона; – адрес электронной почты; – реквизиты документа, удостоверяющего личность; – пол; – гражданство; – адрес регистрации по месту жительства; – информация об оказываемой Услуге (в том числе информация о договоре об оказании услуг и сервисов, информация, содержащаяся в иных документах, формируемых в период оказания услуг и сервисов); – фотоизображение (в случае самостоятельного добавления Пользователем цифрового сервиса в

	приложений и веб-сайтов. 4. Персонализация и улучшение пользовательского опыта - адаптация интерфейса и отображаемого контента под индивидуальные предпочтения пользователя, использование рекомендаций, подсказок и сценариев, настройка уведомлений, тем оформления, отображения модулей и других элементов Цифровых сервисов. 5. Участие в маркетинговых и клиентских программах - реализация программ лояльности, бонусных и акционных предложений, информирование о новых продуктах, изменениях условий обслуживания, проведение опросов, викторин, розыгрышей и иных мероприятий с участием пользователей, а также анализ откликов на рекламные кампании и сегментация аудитории для продвижения Услуг. 6. Взаимодействие с Бизнес-партнёрами - передача данных Бизнес-партнёрам в рамках исполнения договорных обязательств, оказания совместных Цифровых сервисов и обеспечения интеграции цифровых платформ и функционала. 7. Защита прав и законных интересов Компании - реализация прав и законных интересов Компании, включая защиту интересов в рамках досудебных и судебных процессов, а также исполнение требований законодательства.	используемом Цифровом сервисе); - Техническая информация; - Поведенческий профиль; - Финансовая информация.
Исполнители (физические лица) и Уполномоченные представители	1. Заключение и исполнение договоров: - заключение, сопровождение и расторжение договоров (в том числе гражданско-правовых, авторских, подрядных и иных договоров); - ведение расчётов, начислений и выплат, связанных с оказанием услуг или выполнением работ. 2. Проверка соответствия и соблюдение правовых и внутренних требований:	- фамилия, имя, отчество; - дата и место рождения; - реквизиты документа, удостоверяющего личность; - ПИНФЛ; - ИНН; - пол; - гражданство; - адрес регистрации по месту жительства;

	– проведение идентификации и верификации (KYC), включая сбор, проверку и подтверждение сведений и документов; – оценка благонадёжности, профессиональной пригодности, статуса и деловой репутации; – проверка в рамках процедур комплаенса и безопасности, включая санкционные ограничения, конфликт интересов, меры по противодействию отмыванию доходов (AML) и иные ограничения. 3. Организация доступа к ресурсам Компании: – предоставление доступа к информационным системам, офисам и иным объектам Компании в целях исполнения договорных обязательств; – соблюдение внутреннего пропускного режима, правил информационной безопасности и иных режимов доступа. 4. Договорная коммуникация и документооборот: – обработка уведомлений, запросов, претензий, актов, отчётов и другой документации, связанной с исполнением договоров; – взаимодействие по вопросам качества, сроков и условий оказания услуг или выполнения работ. 5. Защита прав и законных интересов Компании: – представление интересов Компании в рамках досудебных и судебных процедур; – подготовка доказательств, переписки, сведений и иных материалов для урегулирования споров или выполнения требований законодательства.	- номер телефона; - адрес электронной почты; - занимаемая должность, наименование организации, сведения о полномочиях; - информация о заключённом договоре (номер, дата, вид договора); - банковские реквизиты.
--	--	---

Работники Компании и их родственники	1. Соблюдение требований законодательства: – исполнение требований трудового, налогового и иного законодательства Республики Узбекистан; – ведение кадрового делопроизводства и личных дел работников; – начисление и выплата заработной платы, налогов и обязательных отчислений; – формирование и подача обязательной отчётности в уполномоченные государственные органы. 2. Обеспечение социального и компенсационного пакета: – оформление и сопровождение медицинского страхования; – оформление абонемента в спортивные залы; – оформление служебной сотовой связи; – выпуск и обслуживание банковских карт для расчётов с работником; – предоставление иных льгот и компенсаций, предусмотренных законодательством и внутренними нормативными документами Компании. 3. Кадровое администрирование и развитие персонала: – формирование и ведение кадрового резерва; – организация переводов внутри Компании; – планирование и сопровождение карьерного роста и профессионального развития; – организация прохождения обучения и повышения квалификации; – организация командировок и служебных поездок.	- фамилия, имя, отчество; - дата и место рождения; - реквизиты документа, удостоверяющего личность; - пол; - ПИНФЛ; - ИНН; - адрес регистрации по месту жительства; - адрес фактического проживания; - номер телефона; - адрес электронной почты; - образование, выполняемая работа с начала трудовой деятельности; - отношение к воинской обязанности, сведения по воинскому учету; - реквизиты платежной карты; - номер индивидуального накопительного пенсионного счета; - семейное положение; - фамилия, имя, отчество и даты рождения близких родственников и реквизиты документов, удостоверяющих личность; - основания прекращения трудового договора; - фотоизображение; - результаты обязательного медицинского осмотра; - сведения, содержащиеся в резюме, анкете или иных
--	---	---

4. Аналитика и статистическая обработка данных:

- сбор, учёт, анализ и подготовка статистической и управленческой отчётности по персоналу;
- прогнозирование потребностей и ресурсов в кадровой сфере.

5. Организация и поддержание внутренней и внешней коммуникации:

- поддержка взаимодействия внутри Компании (в том числе кросс-функциональное и межрегиональное);
- коммуникация с работниками юридических лиц, участниками (акционерами) которых являются VEON Ltd., VEON UZBEKISTAN HOLDING B.V., VEON CENTRAL ASIA B.V. и их аффилированными юридическими лицами;
- взаимодействие с Партнёрами Компании в рамках исполнения договоров и иных обязательств.

6. Реализация прав и защита интересов Компании:

- обеспечение функционирования бизнес-процессов и организации труда;
- контроль выполнения обязанностей и качества работы;
- учёт рабочего времени и оценка эффективности;
- защита имущественных и иных законных интересов Компании;
- участие в досудебных и судебных спорах, рассмотрение обращений и претензий.

7. Обеспечение безопасности:

- обеспечение физической и информационной безопасности, охрана труда;
- защита жизни и здоровья работников;
- защита строго конфиденциальной,

документах, переданных по собственной инициативе;

- биометрические данные: могут обрабатываться для целей управления доступом на территорию и объекты Компании.

	конфиденциальной информации и информации для внутреннего использования; – контроль доступа к помещениям, ресурсам и системам Компании. 8. Контрольные мероприятия – проведение аудита, проверок, ревизий и служебных расследований; – соблюдение внутреннего контроля, антикоррупционных процедур и корпоративной этики.	
Кандидаты на замещение вакантных должностей	1. Подбор и оценка кандидатов: – оценка соответствия квалификации, опыта, компетенций и иных характеристик установленным требованиям Компании; – проверка информации, предоставленной кандидатом, включая рекомендации и иные сведения; – организация и проведение собеседований, оценочных мероприятий и иных этапов подбора персонала. 2. Формирование кадрового резерва. 3. Реализация прав и защита интересов Компании: – разрешение возможных споров, включая досудебное и судебное урегулирование в случае обжалования результатов отбора; – соблюдение внутренних процедур Компании, обеспечивающих прозрачность и обоснованность принятия решений по результатам подбора персонала.	- фамилия, имя, отчество; - дата и место рождения; - реквизиты документа, удостоверяющего личность; - пол; - ПИНФЛ; - гражданство; - номер телефона; - адрес электронной почты; - адрес регистрации по месту жительства; - сведения об образовании, выполняемой работе, квалификации; - фотоизображение; - сведения, содержащиеся в резюме, анкете или иных документах, переданных кандидатом по собственной инициативе.
Стажёры и практиканты Компании	1. Организация и сопровождение стажировки / практики - оформление, проведение и документальное сопровождение стажировки или учебной (производственной) практики в Компании в соответствии с требованиями законодательства и	- фамилия, имя, отчество; - дата и место рождения; - реквизиты документа, удостоверяющего личность;

	внутренними нормативными документами Компании. 2. Доступ и режим пропуска: – оформление пропусков и управление доступом к помещениям и объектам Компании; – соблюдение пропускного режима и мер физической безопасности. 3. Технический и операционный доступ: – предоставление доступа к информационным системам, ресурсам и технической инфраструктуре, необходимым для выполнения задач в рамках стажировки / практики; – соблюдение мер информационной безопасности; – оформление договоров и других соглашений, в том числе для подключения служебной связи и иных корпоративных сервисов. 4. Реализация прав и защита интересов Компании – обеспечение соблюдения требований законодательства РУз; – защита прав в рамках досудебных и судебных процессов.	- пол; - ПИНФЛ; - гражданство; - номер телефона; - адрес электронной почты; - адрес регистрации по месту жительства; - реквизиты платежной карты; - фотоизображение; - сведения, содержащиеся в резюме, анкете или иных документах, переданных по собственной инициативе. - биометрические данные: могут обрабатываться для целей управления доступом на территорию и объекты Компании.
Посетители офисов и объектов Компании	1. Управление доступом и соблюдение пропускного режима: – идентификация и регистрация посетителей; – оформление временных пропусков и контроль доступа на территорию и в помещения Компании; – фиксация времени входа и выхода. 2. Обеспечение физической и информационной безопасности:	- фамилия, имя, отчество; - реквизиты документа, удостоверяющего личность; - дата и время входа/выхода; - цель визита.

- защита жизни и здоровья работников, посетителей и иных лиц, находящихся на территории Компании;
- предотвращение и выявление несанкционированного доступа, правонарушений и иных инцидентов;
- охрана имущества и информационных ресурсов.

3. Реагирование на инциденты и внутренние расследования:

- мониторинг событий безопасности (в том числе с использованием видеонаблюдения);
- проведение служебных проверок в случае нарушений порядка доступа или правонарушений.

4. Реализация прав и законных интересов Компании, включая защиту прав в рамках досудебных и судебных процессов.