ПОЛОЖЕНИЕ
ПО ОРГАНИЗАЦИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ООО «ВТБ Мобайл»

Версия 3.0

г. Москва, 2023 г

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

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.

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

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

1. ОБЩИЕ ПОЛОЖЕНИЯ

Положение по организации обработки и обеспечению безопасности персональных данных в ООО «ВТБ Мобайл» далее – Положение) разработано в соответствии с п. 2 ч. 1 ст. 18.1 Федерального закона № 152–ФЗ «О персональных данных» (далее – ФЗ–152) и определяет порядок обработки персональных данных, а также устанавливает требования к обеспечению безопасности персональных данных, обрабатываемых в ООО «ВТБ Мобайл» (далее – Оператор).

Действия Положения распространяются на обработку персональных данных как с использованием средств автоматизации, так и без использования таких средств.

Нормы и правила, содержащиеся в Положении, являются обязательными для исполнения всеми работниками Оператора, в т. ч. работающими в филиалах и обособленных подразделениях Оператора.

2. ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Назначение ответственных лиц

Для организации обработки и обеспечения безопасности ПДн у Оператора назначаются ответственные лица.

Для организации обработки ПДн назначается Ответственный за организацию обработки ПДн. В своей работе Ответственный за организацию обработки ПДн руководствуется документом «Инструкция ответственного за организацию обработки персональных данных».

2.2 Допуск к персональным данным

Работники Оператора допускаются к обработке ПДн в объеме, необходимом им для выполнения должностных обязанностей.

Перед началом работы с ПДн работники Оператора, допущенные к ПДн, обязаны:

- ознакомиться под подпись с положениями законодательства Российской Федерации о персональных данных (далее – Законодательства);
- ознакомиться под подпись с Положением;
- пройти инструктаж и обучение по работе с ПДн;
- пройти инструктаж и обучение по работе с ПДн в информационных системах ПДн.

Форма Листа ознакомления с порядком обработки персональных данных у Оператора представлена в Приложении № 1 к Положению.

В случае если на основании договоров, заключенных с юридическими или физическими лицами, Оператору необходимо предоставить таким лицам доступ к ПДн, то соответствующие ПДн предоставляются Оператором только после подписания Соглашения об обеспечении безопасности персональных данных, порученных на обработку, или включения в договоры пунктов о конфиденциальности при обработке ПДн.

Государственным органам, осуществляющим функции контроля (надзора), права доступа к ПДн предоставляются только в сфере их компетенции и в объеме, предусмотренном действующим законодательством.

Методы и правила разграничения доступа определяются, исходя из целесообразности и эффективности их применения. Технические средства должны обладать возможностью реализации выбранного метода разграничения доступа.

2.3 Получение персональных данных

ПДн следует получать лично у субъекта ПДн или от его законного представителя. В случае если ПДн возможно получить только у третьей стороны, Оператор до начала обработки таких ПДн

обязан уведомить субъекта ПДн о получении его ПДн. Помимо адреса и наименования организации Оператор должен сообщить субъекту ПДн о целях обработки ПДн, источниках получения и предполагаемых пользователях ПДн, а также сведения о его правах, установленных ФЗ–152.

Оператор освобождается от обязанности предоставить субъекту персональных данных указанные выше сведения, если:

- субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим Оператором;
- ПДн получены Оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн;
- ПДн, разрешенные субъектом для распространения или получены из общедоступного источника;
- Оператор 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 указанных выше сведений нарушает права и законные интересы третьих лиц.

2.4 Передача персональных данных

Передача ПДн субъектов ПДн третьим лицам может осуществляться только при наличии согласия субъекта ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, в целях исполнения условий договора, а также в случаях, установленных законодательством Российской Федерации.

Передача ПДн субъектов между подразделениями Оператора должна осуществляться только между работниками, допущенными к обработке ПДн.

2.5. Трансграничная передача персональных данных

Оператор до начала осуществления деятельности по трансграничной передаче персональных данных обязан уведомить Уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять трансграничную передачу персональных данных по форме, разработанной Уполномоченным органом по защите прав субъектов персональных данных.

Оператор до подачи уведомления о намерении осуществлять трансграничную передачу обязан получить от органов власти иностранного государства, иностранных физических лиц, иностранных юридических лиц, которым планируется трансграничная передача персональных данных, следующие сведения:

- сведения о принимаемых органами власти иностранного государства, иностранными физическими лицами, иностранными юридическими лицами, которым планируется трансграничная передача персональных данных, мерах по защите передаваемых персональных данных и об условиях прекращения их обработки;
- информация о правовом регулировании в области персональных данных иностранного государства, под юрисдикцией которого находятся органы власти иностранного государства, иностранные физические лица, иностранные юридические лица, которым планируется трансграничная передача персональных данных (в случае, если предполагается осуществление трансграничной передачи в иностранные государства, не являющиеся сторонами Конвенции Совета Европы о защите физических лиц при

автоматизированной обработке персональных данных и не включенные в перечень, установленный Приказом Роскомнадзора от 05.08.2022 N 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных»);

– сведения об органах власти иностранного государства, иностранных физических лицах, иностранных юридических лицах, которым планируется трансграничная передача персональных данных (наименование либо фамилия, имя и отчество, а также номера контактных телефонов, почтовые адреса и адреса электронной почты).

По запросу Уполномоченного органа по защите прав субъектов персональных данных Оператор в течение 10 (десяти) рабочих дней с даты получения запроса обязан предоставить в Уполномоченный орган по защите прав субъектов персональных данных сведения, указанные выше. Оператор вправе продлить указанный срок, но не более чем на 5 (пять) рабочих дней при направлении мотивированного уведомления с указанием причин такого продления в Уполномоченный орган по защите прав субъектов персональных данных.

Оператор на основании сведений, полученных от органов власти иностранного государства, иностранных физических лиц, иностранных юридических лиц, которым планируется трансграничная передача персональных данных, обязан до осуществления трансграничной передачи провести оценку соблюдения органами власти иностранных государств, иностранными физическими лицами, иностранными юридическими лицами, которым планируется трансграничная передача персональных данных, конфиденциальности персональных данных и обеспечения безопасности персональных данных при их обработке.

Осуществление трансграничной передачи

Оператор вправе осуществлять трансграничную передачу в государства, не являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и не включенные в перечень, установленный Приказом Роскомнадзора от 05.08.2022 N 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных», по истечении 10 (десяти) рабочих дней после направления уведомления о намерении осуществлять трансграничную передачу в Уполномоченный орган по защите прав субъектов персональных данных в следующих случаях:

– Уполномоченный орган по защите прав субъектов персональных данных не запросил предоставления дополнительных сведений в указанный срок. В случае запроса о предоставлении дополнительных сведений срок рассмотрения уведомления о намерении осуществлять трансграничную передачу Уполномоченным органом по защите прав субъектов персональных данных приостанавливается до даты предоставления Оператором в Уполномоченный орган по защите прав субъектов персональных данных запрошенной информации в соответствии с ч.6, 9 ст. 12 152–ФЗ;

– Уполномоченный орган по защите прав субъектов персональных данных не принял в указанный срок решения о запрете или ограничении трансграничной передачи персональных данных.

Оператор вправе осуществлять трансграничную передачу в государства не являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и не включенные в перечень, установленный Приказом Роскомнадзора от 05.08.2022 N 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных», после подачи уведомления о намерении осуществлять трансграничную передачу в Уполномоченный орган по защите прав субъектов

персональных данных в случае, если такая трансграничная передача необходима для защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц.

В случае намерения осуществлять трансграничную передачу персональных данных в государства, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных или включенных в перечень, установленный Приказом Роскомнадзора от 05.08.2022 N 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных», Оператор вправе осуществлять трансграничную передачу сразу же после направления уведомления о намерении осуществлять трансграничную передачу в Уполномоченный орган по защите прав субъектов персональных данных.

Оператор обязан обеспечить уничтожение органом власти иностранного государства, иностранным физическим лицом, иностранным юридическим лицом ранее переданных им персональных данных в рамках трансграничной передаче персональных данных, в случае принятия Уполномоченным органом по защите прав субъектов персональных данных решения о запрете или ограничении трансграничной передачи персональных данных.

2.5 Хранение персональных данных

Хранение ПДн субъектов осуществляется на бумажных и машинных носителях информации в специально выделенных хранилищах подразделений Оператора, а также в ИСПДн Оператора, обеспечивающих сохранность ПДн и их защиту от несанкционированного доступа.

Уничтожение ПДн в ИСПДн, на машинных и бумажных носителях информации должно производиться в течение 30 (тридцати) дней с даты достижения цели обработки (предельного срока хранения) ПДн. При невозможности уничтожения ПДн в течение тридцати дней с даты достижения цели обработки ПДн обеспечивается их блокирование и уничтожение в срок, не превышающий 6 (шести) месяцев.

Порядок уничтожения ПДн для каждой цели обработки закреплен в Перечне процессов обработки персональных данных и сведения об их обработке.

Оператор при уничтожении персональных данных должен оформить документ, подтверждающий уничтожение персональных данных.

В случае если обработка персональных данных осуществляется Оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является Акт об уничтожении персональных данных.

В случае если обработка персональных данных осуществляется Оператором с использованием средств автоматизации либо одновременно с использованием средств автоматизации и без использования средств автоматизации документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются Акт об уничтожении персональных данных и Выгрузка из журнала регистрации событий в информационной системе персональных данных (далее – Выгрузка из журнала).

Акт об уничтожении персональных данных должен содержать:

– наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица) и адрес оператора;

– наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица), адрес лица (лиц), осуществляющего (осуществляющих) обработку персональных данных субъекта (субъектов) персональных данных по поручению оператора (если обработка была поручена такому (таким) лицу (лицам);

– фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

– фамилию, имя, отчество (при наличии), должность лиц (лица), уничтоживших персональные данные субъекта персональных данных, а также их (его) подпись;

– перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

– наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) персональные данные субъекта (субъектов) персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);

– наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);

– способ уничтожения персональных данных;

– причину уничтожения персональных данных;

– дату уничтожения персональных данных субъекта (субъектов) персональных данных.

Акт об уничтожении персональных данных может быть подписан как в бумажной форме, так и в электронной форме в соответствии с требованиями Федерального закона от 06.04.2011 N 63–ФЗ «Об электронной подписи».

Выгрузка из журнала должна содержать:

– фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

– перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

– наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных;

– причину уничтожения персональных данных;

– дату уничтожения персональных данных субъекта (субъектов) персональных данных.

В случае если выгрузка из журнала не позволяет указать отдельные сведения, указанные выше, недостающие сведения вносятся в Акт об уничтожении персональных данных.

Акт об уничтожении персональных данных и Выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.

Настоящий пункт не применяется к подтверждению уничтожения персональных данных, содержащихся в архивных документах, в соответствии с законодательством об архивном деле в Российской Федерации.

2.6 Уведомление об обработке персональных данных

Согласно ст. 22 ФЗ–152 Оператор уведомляет Уполномоченный орган по защите прав субъектов персональных данных об обработке ПДн.

В случае изменения сведений, указанных в уведомлении, а также в случае прекращения обработки ПДн Оператор также уведомляет об этом Уполномоченный орган по защите прав

субъектов персональных данных не позднее 15–го числа месяца, следующего за месяцем, в котором возникли такие изменения или прекратилась обработка ПДн.

3. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

Работники Оператора, осуществляющие обработку ПДн без использования средств автоматизации, должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки.

ПДн при их обработке без использования средств автоматизации обособляются от иной информации путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

При фиксации ПДн на материальных носителях не допускается запись на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы. При обработке различных категорий ПДн без использования средств автоматизации для каждой категории ПДн должен использоваться отдельный материальный носитель.

При использовании типовых форм документов характер информации, в которых предполагает или допускает включение в них ПДн, должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, наименование и адрес Оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;

– типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, при необходимости получения письменного согласия на обработку ПДн;

– типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

– типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн.

Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

Уничтожение, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

Уточнение ПДн при их обработке без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, то путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна производиться таким образом, чтобы можно было определить места хранения персональных данных (материальных носителей).

4. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Организация защиты персональных данных

Оператор при обработке ПДн обязан принимать 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.

Для обеспечения безопасности ПДн применяются следующие меры:

- определение угроз безопасности ПДн при их обработке в ИСПДн;
- применение 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;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- ведение учета машинных носителей ПДн;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

ПДн обрабатываются у Оператора как с использованием средств автоматизации, так и без использования таких средств.

В отсутствие работника на его рабочем месте не должно быть документов и машинных носителей информации, содержащих ПДн.

Доступ работников Оператора и иных лиц в помещения, в которых осуществляется обработка и хранение ПДн, ограничивается организационными мерами.

Организацию обработки ПДн субъектов и контроль соблюдения мер их защиты в структурных подразделениях Оператора, работники которых имеют доступ к ПДн, осуществляют их непосредственные руководители.

Организация защиты ПДн, обрабатываемых в ИСПДн, осуществляется в рамках действующей системы защиты.

Разработка и осуществление мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн, может осуществляться сторонними организациями на договорной основе, в том числе имеющими лицензии на право проведения соответствующих работ в случаях, предусмотренных требованиями законодательства Российской Федерации.

4.2 Обеспечение безопасности персональных данных при взаимодействии Оператора с третьими лицами

В целях обеспечения безопасности ПДн при взаимоотношении Оператора с третьими лицами должны выполняться следующие меры:

- должно быть подписано Соглашение об обеспечении безопасности персональных данных, порученных на обработку;
- должен проводиться мониторинг действий третьих лиц в ИСПДн Оператора.

В случае заключения с юридическим лицом договора, одним из условий которого является передача юридическому лицу персональных данных, обрабатываемых Оператором на законных основаниях, Оператор должен удостовериться до заключения договора в адекватном уровне обеспечения юридическим лицом безопасности ПДн. Обязательным является предоставление третьим лицом гарантий выполнения действующего законодательства Российской Федерации в области обеспечения безопасности ПДн.

Любое соединение с внешней информационной системой должно быть согласовано с, ответственным за организацию обработки ПДн и ответственным за обеспечение безопасности ПДн в информационных системах. Любой доступ должен быть ограничен и протестирован на возможные уязвимости. Внешний доступ должен также отвечать следующим характеристикам:

- необходимо подписание владельцем внешней информационной системы соглашения о принятии на себя обязательств по обеспечению безопасности ПДн в своей части сети, соединенной с сетью Оператора;
- должен быть обеспечен контроль доступа и аутентификация.

5. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

За неисполнение или ненадлежащее исполнение работником возложенных на него обязанностей по соблюдению установленного порядка работы с ПДн работодатель вправе применять предусмотренные Трудовым кодексом Российской Федерации № 197–ФЗ дисциплинарные взыскания.

Ответственность за несоблюдение вышеуказанного порядка обработки ПДн несет работник, а также руководитель структурного подразделения, осуществляющего обработку ПДн.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, могут быть привлечены к административной и уголовной ответственности в порядке, установленном федеральным законодательством Российской Федерации.

6. ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ

Пересмотр Положения осуществляется в следующих случаях:

- при появлении новых требований к обработке и обеспечению безопасности ПДн со стороны российского законодательства и государственных органов, осуществляющих функции контроля (надзора);
- по результатам проверок государственных органов, осуществляющих функции контроля (надзора), выявивших несоответствия требованиям по обработке и обеспечению безопасности ПДн;
- по результатам внутреннего контроля (аудита) системы защиты ПДн в случае выявления существенных нарушений;

– по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн и выявивших недостатки в правилах предоставления доступа к ПДн.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Повседневный контроль порядка обращения с ПДн осуществляют руководители тех структурных подразделений Оператора, в которых обрабатываются ПДн.

Периодический контроль выполнения Положения возлагается на ответственного за организацию обработки ПДн и ответственного за обеспечение безопасности ПДн в информационных системах.