

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Киев, 2019 г.

СОДЕРЖАНИЕ

1	ОБЩИЕ ПОЛОЖЕНИЯ	3
2	СУБЪЕКТЫ И ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	5
3	ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	6
3.1	Назначение ответственных лиц.....	6
3.2	Допуск работников к обработке персональных данных.....	6
3.3	Получение персональных данных	6
3.4	Систематизация, накопление, уточнение и использование персональных данных	7
3.5	Передача персональных данных	7
3.6	Хранение персональных данных	7
3.7	Уведомление об обработке персональных данных.....	7
4	ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ.....	9
5	ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ	11
6	ПОРЯДОК ОБРАБОТКИ ОБРАЩЕНИЙ И ЗАПРОСОВ ПО ВОПРОСАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	12
7	ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	13

1 ОБЩИЕ ПОЛОЖЕНИЯ

Положение об обработке персональных данных в ООО «СПА ФИНАНС» (далее – Положение) разработано в соответствии с законодательством Украины, Трудовым кодексом Украины (далее – ТК Украины), а также «Перечнем сведений конфиденциального характера», утвержденным Указом Президента Украины от 06.03.1997 № 188.

Настоящее Положение определяет порядок обработки персональных данных и устанавливает общие требования к обеспечению безопасности персональных данных, обрабатываемых в ООО «СПА ФИНАНС» (далее – Оператор) как с использованием средств автоматизации, так и без использования таких средств.

В Положении используются следующие основные понятия:

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

обезличивание персональных данных – действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному 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;

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту 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 (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу;

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.

Действие Положения распространяется на все структурные подразделения Оператора.

Настоящее Положение должно быть доведено до каждого работника Оператора, осуществляющего обработку персональных данных, под роспись.

2 СУБЪЕКТЫ И ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Цели обработки персональных данных, основания для их обработки, возможные действия (операции), совершаемые с персональными данным, сроки обработки и состав обрабатываемых персональных категорий субъектов персональных данных, обрабатываемых у Оператора, указаны в Перечне обрабатываемых персональных данных.

3 ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Назначение ответственных лиц

Для организации обработки персональных данных у Оператора назначается ответственное лицо.

Для определения уровня защищенности информационных систем персональных данных, проверки готовности средств защиты информации к использованию, а также уничтожения персональных данных приказом руководителя Оператора назначается Комиссия по приведению в соответствие с требованиями законодательства Украины в области персональных данных (далее – Комиссия).

В своей работе Комиссия руководствуется Положением о комиссии по приведению в соответствие с требованиями законодательства Украины в области персональных данных, утвержденным приказом руководителя Оператора.

3.2 Допуск работников к обработке персональных данных

Допуск работников Оператора к обработке персональных данным осуществляется на основании приказа о назначении на должность в соответствии с Перечнем должностей и третьих лиц, имеющих доступ к персональным данным.

Работники Оператора получают доступ к обработке персональных данных для выполнения ими служебных (трудовых) обязанностей, после выполнения следующих мероприятий:

- ознакомления под роспись с руководящими документами Оператора и нормативными актами Украины по обработке и обеспечению безопасности персональных данных;
- оформления письменного обязательства о неразглашении персональных данных, форма которого утверждена приказом руководителя Оператора.

Работники Оператора, имеющие допуск к персональным данным, имеют право получать только те персональные данные, которые необходимы им для выполнения служебных (трудовых) обязанностей.

3.3 Получение персональных данных

Персональные данные субъекта получаются от него самого или от него законного представителя. В случае, если персональные данные получены не от субъекта персональных данных, Оператор до начала обработки таких персональных данных обязан уведомить субъект о получении его персональных данных.

3.4 Систематизация, накопление, уточнение и использование персональных данных

Систематизация, накопление, уточнение и использование персональных данных осуществляется путем оформления и ведения документов учета и баз данных субъектов персональных данных.

Работники Оператора, имеющие доступ к персональным данным, должны обеспечить их обработку, исключая несанкционированный доступ к ним третьих лиц.

3.5 Передача персональных данных

Передача персональных данных субъектов третьим лицам может осуществляться только при наличии письменного согласия субъекта, если иное не предусмотрено федеральным законодательством.

При передаче персональных данных субъектов третьим лицам, с третьим лицом должно быть подписано Соглашение о соблюдении безопасности персональных данных, переданных на обработку, форма которого утверждена приказом руководителя Оператора.

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

3.6 Хранение персональных данных

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

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

Порядок и правила учета, хранения и уничтожения персональных данных описаны в Регламенте по учету, хранению и уничтожению носителей персональных данных.

3.7 Уведомление об обработке персональных данных

Согласно законодательству Оператор уведомляет Уполномоченный орган по защите прав субъектов персональных данных об обработке персональных данных.

В случае изменения сведений, указанных в уведомлении, а также в случае прекращения обработки персональных данных Оператор также уведомляет об этом Уполномоченный орган.

4 ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

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

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

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

- типовая форма должна содержать сведения о цели обработки персональных данных, наименование и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных – при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

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

Необходимо обеспечивать отдельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

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

Уточнение персональных данных 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, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы:

- о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации;
- о категориях обрабатываемых персональных данных;
- об особенностях и правилах осуществления такой обработки.

5 ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

Порядок обработки и защиты персональных данных в информационных системах Оператора определяется Положением об обеспечении безопасности персональных данных.

Защита персональных данных от неправомерного их использования или утраты обеспечивается Оператором за счет собственных средств.

Работники Оператора, которые в рамках исполнения должностных обязанностей имеют доступ к персональным данным, обязаны соблюдать режим конфиденциальности персональных данных на всех этапах их обработки.

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

Доступ работников Оператора и иных лиц в помещения, в которых осуществляется обработка и хранение персональных данных, ограничивается организационными мерами и применением системы контроля и управления доступом.

Учитывая массовость и единые места обработки и хранения, гриф «конфиденциально» на документах, содержащих персональные данные, не ставится.

Организацию обработки персональных данных субъектов, контроль соблюдения мер их защиты в структурных подразделениях Оператора, сотрудники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

Мероприятия по защите персональных данных осуществляются в соответствии с Планом мероприятий по приведению в соответствие с требованиями законодательства Украины в области персональных данных, утверждаемых руководителем Оператора.

Разработка и осуществление мероприятий по обеспечению безопасности персональных данных, обрабатываемых в информационных системах, может осуществляться сторонними организациями на договорной основе, имеющими лицензии на право проведения соответствующих работ.

6 ПОРЯДОК ОБРАБОТКИ ОБРАЩЕНИЙ И ЗАПРОСОВ ПО ВОПРОСАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Порядок обработки запросов субъектов персональных данных описан в Регламенте по реагированию на запросы субъектов персональных данных.

Порядок обработки запросов уполномоченных органов в области персональных данных описан в Регламенте по взаимодействию с органами государственной власти в области персональных данных.

7 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Иные права и обязанности работников, в функции которых входит обработка персональных данных, определяются Инструкцией пользователя информационных систем персональных данных.

Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

Разглашение персональных данных, их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, другими локальными нормативными актами (приказами, распоряжениями) Оператора, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарного взыскания – замечания, выговора, увольнения.

Работник, имеющий доступ к персональным данным и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба работодателю.

Работники Оператора, имеющие доступ к персональным данным, виновные в их незаконном разглашении или использовании без согласия субъектов персональных данных из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии с законодательством Украины.

Обновление и актуализация настоящего положения осуществляется в соответствии с Регламент по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности.

