АСКОН НАВИГАТОР

Электронный журнал для специалистов в области бухгалтерии, кадров и права

Файл сформирован 26.04.2024

Маленькие аспекты больших данных: частые ошибки при передаче персональных данных и как их исправить

Цифровизация, безбумажное документирование трудовых отношений определяют необходимость присмотреться к привычным и отработанным технологиям работы с персональными данными и иными законом защищаемым сведениям, заблаговременно обеспечив точное соблюдение требований регулятора. Уже сейчас следует выверить все этапы оформления трудовых отношений, исключив все возможности нарушения действующего законодательства.

«Слабые звенья» передачи персональных данных

Сегодня особого внимания заслуживают распространенные «слабые звенья» передачи информации, такие как:

- взаимодействие кадрового подразделения с бухгалтерией (централизованной, обособленной, удаленной) и иными отделами предприятия;
- документирование труда удаленных работников;
- предоставление сведений в государственные информационные системы.

Взаимодействие с бухгалтерией (централизованной, обособленной, удаленной) и иными подразделениями предприятия зачастую осуществляется без особых мер предосторожности, словно передача информации происходит между двумя физическими лицами в изолированном помещении. Эта иллюзия создается привычным выполнением работником своей рутинной трудовой функции на своем рабочем месте. Но многие рабочие места организуются в виде удаленных рабочих столов, подключаемых к компьютеру с использованием системы идентификации пользователя в определенной сети. И не многие работники задаются вопросами:

- кто пользуется этим компьютером еще;
- кто организует функционирование сети, соединяющей данный рабочий стол с этим компьютером;
- какие уязвимости и угрозы существуют в этой информационной среде и каналах связи.

Это влечет нарушения безопасности информационной среды. Обрабатывая персональные данные каждый пользователь как оператор (физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных) обязан обеспечить не только сохранность сведений на всех этапах их обработки, но и во время эксплуатации технических средств, использования программного обеспечения и передачи данных с одного компьютера на другой.

Какие ограничения необходимо учитывать отделу кадров

Нельзя передавать персональные данные без их из защиты, например, паролем, просто прикрепляя файл с информацией к письму.

Нельзя использовать общие, публичные интернет соединения в метро, кафе, образовательных организаций для передачи персональных данных.

Нельзя отправлять и получать персональные данные с использованием почтового ящика поисковой системы и интернет-портала.

Эти и другие ограничения действий оператора как контролируемого лица, самостоятельно или совместно с другими контролируемыми лицами организующее и (или) осуществляющее обработку персональных

данных, в том числе на основании поручения, определены Постановлением Правительства РФ от 29.06.2021 N 1046 "О федеральном государственном контроле (надзоре) за обработкой персональных данных" (вместе с "Положением о федеральном государственном контроле (надзоре) за обработкой персональных данных")

Аналогичные ограничения действуют и при документировании деятельности, при взаимодействии с удаленными работниками. Работодатель обязанне только предусмотреть, регламентировать локальными актами все особенности работы с персональными данными, но и организовать работу по контролю исполнения требований.

Где необходимо провести ревизию

Способы обработки персональных данных, перечень данных и другие специфические особенности обмена информации определяют и перечень объектов, подлежащих ревизии. Общей для всех можно считать необходимость актуализировать:

- локальные акты об обработке законом защищаемых сведений;
- документы, определяющие функционирование информационных систем и порядок выявления утечек, хищения, несанкционированного доступа к защищаемым сведениям;
- документы, определяющие права и обязанности каждого работника, осуществляющего действия с информацией (например, обязательство о неразглашении персональных данных, политику организации идентификации и доступа пользователей в информационную систему);
- трудовые договоры работников

Отдельного упоминания заслуживают требования предоставления услуг мобильной связи только тем абонентам (и пользователям услуг связи тех абонентов), достоверные сведения о которых будут сообщены оператору связи и внесены в его автоматизированную систему расчетов. Соответственно, работодатель обязан предоставлять оператору связи персональные данные работника, получившего корпоративную SIM-карту мобильной связи. Но сделать это можно только при наличии соответствующего согласия работника как субъекта персональных данных.

Кроме того, следует обратить внимание на порядок действий ответственного лица при внесении сведений в государственные информационные системы. Необходимость ревизии и контроля соблюдения требований к обработке и передачи персональных данных подкрепляется увеличением информации, передаваемой работодателем и в государственные информационные системы.

Привычный обмен данными с налоговой инспекцией, фондом социального страхования, пенсионным фондом обрастает необходимостью внесения данных в портал «Работа в России» (Постановление Правительства РФ от 25.08.2015 N 885 "Об информационно-аналитической системе Общероссийская база вакансий "Работа в России" (вместе с "Правилами формирования, ведения и модернизации информационно-аналитической системы Общероссийская база вакансий "Работа в России") и необходимостью использования информационной системы Роскомнадзора для контроля распространения персональных данных.

Сложно предположить взаимозависимость этих событий, но нельзя не учитывать их время начала и время окончания. Тем более, что утвержденные Правила (Приказ Роскомнадзора от 21.06.2021 N 106 "Об утверждении Правил использования информационной системы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в том числе порядка взаимодействия субъекта персональных данных с оператором") определяют в том числе порядок взаимодействия субъекта персональных данных с оператором для получения последним согласия на обработку персональных данных, которые субъект разрешил распространять (п. 1 Правил), а распространение персональных данных подразумевает, что:

- субъект персональных данных подписывает согласие электронной подписью (п. 4 Правил);
- подсистема Единой системы идентификации и аутентификации, содержит данные перечня записей о предоставленных и отозванных согласиях, позволяющие Роскомнадзору реагировать на поступившее обращение о нарушении прав субъекта персональных данных (п. 2 Правил).

Соответственно, вопросы действий оператора с персональными данными (распространение или предоставление сведений), техническое и программное обеспечение этих действий, не только находят свое актуальное регулирование, но и вносят новые значения и алгоритмы в привычные процедуры обработки информации, определяя конечного пользователя, исполнителя ответственным за все свои действия с персонализацией ответственностью.