АСКОН НАВИГАТОР

Электронный журнал для специалистов в области бухгалтерии, кадров и права

Файл сформирован 29.03.2024

Обработка личных сведений при оказании услуг: хотят запустить сервис по отзыву согласий

Минцифры предлагает создать реестр согласий на обработку персональных данных. Речь идет о согласиях, которые дают, чтобы получить разные услуги, вступить в программы лояльности и т.д. Вероятно, гражданин сможет в личном кабинете Госуслуг:

- видеть свои согласия, их даты и адресатов;
- получать доступ к составу личных сведений, которые есть у операторов;
- отзывать согласия;
- контролировать удаление персональной информации.

Если дать новое согласие, данные о нем попадут на Госуслуги автоматически.

Глава государства идею поддержал (с. 20 информации с сайта президента).

Сейчас на Госуслугах можно отзывать электронные согласия, которые передали через этот портал.

Документы: Информация Минцифры России от 01.09.2022, Информация с сайта Президента РФ от 31.08.2022

Читайте эту новость в КонсультантПлюс

Полезное в КонсультантПлюс по теме

Какие изменения учесть при работе с персональными данными с 1 сентября, всю информацию вы найдете в обзоре экспертов КонсультантПлюс.

Возможно, вам будут интересны эти темы:

ПРОФРАЗВИТИЕ

СТАТЬИ

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

Дата публикации: 2021-10-08 09:00:00

Автор:

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.

СТАТЬИ

Обязанности работодателя по противоэпидемическим мероприятиям: как

передавать персональные данные работников

Дата публикации: 2021-07-19 09:00:00

Автор:

В соответствии с Постановлением Правительства Санкт-Петербурга от 13.03.2020 N 121 (ред. от 19.06.2021) на работодателе лежит обязанность по актуализации информации о работниках, переведенных на дистанционный режим работы (с соблюдением требований законодательства о персональных данных), путем направления информации через личный кабинет на сайте СПб ГБУ "Центр развития и поддержки предпринимательства". В соответствующей форме, размещенной в личном кабинете, содержится таблица, которую необходимо заполнить в том числе номерами телефонов работников.

Но возникает вопрос. Учитывая положения законодательства о персональных данных, вправе ли работодатель без получения согласия работника направить через личный кабинет данные о его номере телефона ?

С точки зрения законодательства о персональных данных

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 Закона о персональных данных).

Как разъясняет Минкомсвязи, абонентский номер или адрес электронной почты могут быть признаны персональными данными в случае, когда такая информация относится прямо или косвенно к определенному или определяемому физическому лицу. Например, абонентский номер, принадлежащий юридическому лицу, не может рассматриваться в качестве персональных данных.

Закон о персональных данных устанавливает, что обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. При этом предусмотрены случаи, когда допускается обработка персональных данных без согласия субъекта персональных данных. В частности, допускается обработка персональных данных, которая необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.

Из судебной практики следует, что номер мобильного телефона относится к персональным данным даже без указания иных данных, позволяющих идентифицировать физическое лицо.

Как установлено в статье 88 ТК РФ, при передаче персональных данных работника работодатель должен соблюдать требования о запрете сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами.

Обязанности работодателя при режиме повышенной готовности

Но при этом надо учитывать особенности режима повышенной готовности.

Органы управления и силы единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций функционируют в режиме повышенной готовности - при угрозе возникновения чрезвычайной ситуации.

В случае угрозы возникновения и распространения инфекционных заболеваний предусмотрено введение ограничительных мероприятий (карантина) на территории Российской Федерации, территории соответствующего субъекта Российской Федерации, муниципального образования, в организациях и на

объектах хозяйственной и иной деятельности

К ограничительным мероприятиям (карантину) относятся административные, медико-санитарные, ветеринарные и иные меры, направленные на предотвращение распространения инфекционных заболеваний и предусматривающие особый режим хозяйственной и иной деятельности, ограничение передвижения населения, транспортных средств, грузов, товаров и животных.

Правительство Санкт-Петербурга имеет право устанавливать обязательные для исполнения гражданами и организациями правила поведения при введении режима повышенной готовности или чрезвычайной ситуации. Эти правила поведения (санитарно-противоэпидемические мероприятия) должны соответствовать нормам законодательства о санитарно-эпидемиологическом благополучии населения. Точного их перечня не существует, уполномоченные органы их разрабатывают, исходя из ситуации. При этом, под санитарно-противоэпидемическими (профилактическими) мероприятиями понимаются организационные, административные, инженерно-технические, медико-санитарные, ветеринарные и иные меры, направленные на устранение или уменьшение вредного воздействия на человека факторов среды обитания, предотвращение возникновения и распространения инфекционных заболеваний и массовых неинфекционных заболеваний (отравлений) и их ликвидацию.

Постановление Правительства Санкт-Петербурга от 13.03.2020 N 121 (ред. от 19.06.2021) издано во исполнение указанных прав и в соответствии с законодательством о защите граждан от чрезвычайных ситуаций природного и техногенного характера.

В соответствии с пунктом 2-41, 2-52 Постановления Правительства Санкт-Петербурга от 13.03.2020 N 121 (ред. от 13.06.2021) организациям (индивидуальным предпринимателям) предписано обеспечить направление списка телефонных номеров работников (исполнителей по гражданско-правовым договорам), указанных в абзаце первом пункта 2-42 постановления, не переведенных на дистанционный режим работы, а также актуализировать информацию, в случае изменения количества работников (исполнителей по гражданско-правовым договорам), не переведенных на дистанционный режим работы, в течение трех дней со дня указанного изменения.

Таким образом, номера телефонов, зарегистрированные на сотрудников, являются персональными данными и, по общему правилу, работодателю необходимо согласие на их обработку. Однако, поскольку передача таких персональных данных в Центр развития предпринимательства предусмотрена постановлением Правительства Санкт-Петербурга, принятым во исполнение Федерального закона "О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера", то можно сделать вывод, что в приведенной ситуации согласия работников не требуется. При этом каких-либо официальных разъяснений или судебной практики по соответствующим случаям нет.