

# COVID-19 и обработка персональных данных

## 1/15/20

В связи с объявленной в Латвии чрезвычайной ситуацией в целях ограничения распространения коронавирусной инфекции COVID-19 предприятия, а также государственные и муниципальные учреждения приняли меры для защиты работников, клиентов и других лиц от вероятной угрозы их здоровью, чтобы в то же время продолжать работу в возможном объеме, учитывая установленный режим чрезвычайной ситуации. С учетом новых обстоятельств дополнительно осуществляется сбор и обработка нового вида информации о физических лицах: например, наблюдаются ли у них симптомы коронавирусной инфекции, контактировал ли человек с возможно инфицированным, включая любые связанные с COVID-19 проверки и их результаты, а также другую информацию, связанную с местами, которые человек посещал.

Указанные сведения, собираемые предприятиями, являются персональными данными, в том числе персональными данными особых категорий, о физических лицах, поддающихся идентификации, и к обработке таких данных предъявляются строгие требования согласно Общему регламенту о защите данных (ОРЗД). В настоящей статье – о важнейших вопросах, которые предприятиям необходимо учитывать в ходе обработки данных физических лиц в связи с выявлением и ограничением распространения COVID-19.

### Что обязательно нужно принять во внимание

В первую очередь необходимо учитывать, что информация, полученная от физических лиц в связи с COVID-19, большей частью считается персональными данными особых категорий, поскольку согласно части первой статьи 9 ОРЗД сведения о здоровье физического лица признаются персональными данными особых категорий.

Учитывая ситуацию, сложившуюся сейчас в Латвии и в мире, в целях ограничения и уничтожения COVID-19 предприятиям разрешается обрабатывать вышеупомянутые персональные данные, однако при этом необходимо обеспечить предусмотренное в ОРЗД оповещение субъектов данных (физических лиц), поскольку сейчас, с учетом особых обстоятельств в связи с COVID-19, предприятие может собирать информацию, которую раньше не получало и которая непосредственно не связана с обеспечением деятельности предприятия, однако текущим основанием для получения такой информации от физических лиц является COVID-19. К примеру, предприятие может дополнительно собирать информацию о том, является ли работник постоянно изолированным, сведения о температуре тела работников и посетителей помещений, а также другие сведения, если предприятие может обосновать, что данные сведения относятся к ограничению распространения COVID-19, защите и обеспечению жизни и здоровья других физических лиц.

К обработке персональных данных, в особенности данных особых категорий, предъявляются строгие требования, предусмотренные в ОРЗД и национальных нормативных актах, и предприятие в качестве администратора обработки персональных данных во время получения информации о физических лицах несет полную ответственность за законность ее обработки согласно требованиям ОРЗД.

Во-вторых, предприятия должны понимать и четко определить, какие персональные данные и

персональные данные особых категорий они получают от физических лиц согласно целям, поставленным предприятиями и в общем определенным в стране в связи с ограничением распространения COVID-19. В противном случае существует вероятность, что предприятие получает слишком много персональных данных, что может быть незаконно и в нынешних условиях. В ОРЗД недвусмысленно указано, что разрешается собирать лишь такое количество информации о физическом лице, которое абсолютно необходимо для достижения поставленных целей.

Перед началом сбора любых данных от физических лиц предприятие должно иметь ясную цель и понимание относительно того, какие персональные данные и персональные данные особых категорий необходимы для достижения определенной цели, в основе которой лежит ограничение распространения COVID-19.

К примеру, если предприятие принимает решение, что работник должен находиться на домашней изоляции, может оказаться достаточным задать вопрос, есть ли у данного работника или кого-либо из его домочадцев симптомы COVID-19 (вместо запроса подробной и специфической информации).

Придерживаясь такого подхода, предприятие выполнит предусмотренный в ОРЗД принцип минимизации данных, а также предотвратит хранение излишней информации о работниках, рискуя существенно нарушить ОРЗД. В то же время предприятие должно обеспечить, чтобы информация, полученная о физических лицах в период ограничения распространения COVID-19, хранилась лишь до тех пор, пока существует цель обработки персональных данных.

В-третьих, предприятию необходимо соответствующее юридическое основание для обработки персональных данных, полученных в связи с COVID-19. Согласно ОРЗД, чтобы обеспечить себе юридическое основание для обработки персональных данных в контексте COVID-19, предприятие может полагаться на следующие правомерные основания для обработки данных:

- *Легитимные интересы.* Предприятие может считать необходимым обрабатывать персональные данные, относящиеся к работнику и другим связанным с ним физическим лицам, чтобы защитить свои законные интересы, связанные с непрерывностью предпринимательской деятельности и выполнением своих обязанностей перед физическими лицами, которые напрямую зависят от способности предприятия, к примеру, обеспечивать рабочие места или предоставлять услуги клиентам. Предприятие должно понимать, имеют ли его интересы в ходе обработки персональных данных преимущество перед интересами, основными правами и свободами указанных лиц. Поэтому рекомендуется провести тест на сравнение интересов в связи с обработкой такого рода персональных данных, которую предприятие осуществляет или планирует.
- *Выполнение договора.* Если обработка персональных данных, связанных с COVID-19, необходима предприятию для выполнения его обязательств перед работниками согласно трудовому договору (явным или подразумеваемым условиям), к примеру, обязанности обеспечивать здоровье, безопасность и благополучие работников, такая обработка может быть обоснована выполнением договора.
- *Юридическая обязанность.* В зависимости от применимых нормативно-правовых актов у предприятия могут быть юридические обязательства относительно здоровья и безопасности, а также существует возможность, что внешним нормативным актом предусматривается обязанность предприятия осуществлять конкретные действия по обработке персональных данных, которые могут быть обоснованы законной обязанностью предприятия.

Однако, несмотря на возможное наличие у предприятия юридического (законного) основания обрабатывать вышеуказанные персональные данные, на него распространяются предусмотренные в ОРЗД обязанности предприятия в качестве администратора, к примеру, обязанность информировать и осуществление соответствующих технических и организационных мероприятий, которые не отменяются и в момент, когда мире происходит борьба с распространением COVID-19. Даже если в настоящий момент надзорное учреждение «закрывает глаза» на возможные нарушения в ходе обработки данных, предприятию необходимо считаться с тем, что, если Государственная инспекция данных обнаружит, что обработка данных была незаконной или в ходе обработки данных не соблюдались предусмотренные в ОРЗД требования, она наложит штраф даже через какое-то время после совершения или обнаружения нарушения, ввиду чего предприятию не стоит полагаться на то, что возможные нарушения защиты данных во время чрезвычайной ситуации, если такие будут обнаружены, останутся безнаказанными.

## Обязанности предприятия

Несомненно, сейчас предприятия заняты другими проблемами и осуществляемые процессы обработки персональных данных могут быть последним поводом для беспокойства, но все же, чтобы предприятиям после преодоления кризиса COVID-19 не пришлось столкнуться с новыми проблемами, уже сейчас, используя имеющихся работников, можно предпринять некоторые действия, чтобы обеспечить законность обработки персональных данных, осуществляемой с целью ограничить распространение COVID-19 и бороться с вызванными им последствиями.

Предприятиям рекомендуется и в это время по необходимости пересматривать и обновлять уведомления о конфиденциальности. Пересмотр имеющихся уведомлений о конфиденциальности важен, чтобы удостовериться в том, что они содержат необходимую информацию о полученных данных и целях обработки предприятием конкретных данных. Если предприятие получает от физических лиц новые категории персональных данных или персональные данные особых категорий и использует их в новых целях, может потребоваться обновление уведомлений о конфиденциальности, чтобы отразить изменения в процессе получения данных от физических лиц.

С точки зрения обеспечения защиты данных предприятиям также стоит рассмотреть ряд других вопросов, в том числе о разглашении случаев заболевания COVID-19 другим работникам предприятия. В рамках обязанности предприятия обеспечивать здоровье и безопасность работников работодатели могут, соблюдая требования применимого законодательства, информировать работников о случаях заболевания COVID-19. Разглашение такой информации следует по возможности ограничивать. В случае необходимости разгласить имя работника, у которого, к примеру, обнаружено заболевание COVID-19 (и это иным путем разрешено применимыми нормативно-правовыми актами), чтобы другие работники могли принять соответствующие защитные меры, работника, чьи данные планируется предать гласности, вначале необходимо уведомить о разглашении его данных, одновременно предотвращая чрезмерное разглашение данных и разглашение лицам, которые не должны получать такие сведения.

Если предприятие получает запрос субъекта данных, однако с учетом нынешней ситуации все усилия и внимание предприятия сосредоточены на устранении последствий вспышки COVID-19, то и в этом случае необходимо позаботиться о соблюдении сроков предоставления ответа на запрос субъекта данных. Если предприятие опасается, что не сможет соблюсти предусмотренные в ОРЗД сроки, следует как можно скорее сообщить об этом субъекту данных, указав, что ответ на запрос будет подготовлен по возможности быстрее, однако с учетом обстоятельств он не будет

предоставлен в установленный срок.

Предприятию рекомендуется рассмотреть возможность провести оценку влияния на защиту данных, поскольку в статье 35 ОРЗД это считается обязательным действием в случае обработки конкретных данных. Согласно ОРЗД, предприятию необходимо провести оценку влияния, если обработка может подвергнуть права и свободы лиц значительному риску. Оценка влияния предназначена для того, чтобы помочь предприятию осознать риски, связанные с конкретными действиями по обработке данных, и меры, которые оно может принять, чтобы ограничить такие риски. Кроме того, оценка влияния поможет информировать об изменениях, которые может потребоваться внести в другой документ соответствия, связанный с защитой данных на предприятии (например, уведомления о конфиденциальности и регистр действий по обработке).

## Стоит подумать

С учетом нынешней ситуации предприятиям особенно важно тщательно следить за безопасностью систем и киберугрозами. И персональные данные, и персональные данные особых категорий следует надлежащим образом защищать, в особенности обрабатываемые медицинские данные, и меры безопасности для защиты таких данных должны применяться строже. Кроме того, предприятия должны удостовериться в том, что они продолжают соблюдать сроки оповещения надзорных учреждений (а также частных лиц в случае необходимости) о нарушениях в области защиты персональных данных, если с учетом тяжести нарушения в ОРЗД предусматривается обязанность информирования.

В то же время мы советуем оценить необходимость заключить с вовлеченными третьими сторонами (например, поставщиками ИТ-услуг или медицинских услуг) договоры об обработке данных.

То, что сейчас предприятиям сложно соблюдать все необходимые стандарты защиты данных, поскольку ресурсы направлены на ограничение распространения COVID-19, понимают и надзорные учреждения; некоторые из них отметили, что к предприятиям, неспособным в настоящий момент обеспечить выполнение своих обязательств, не следует применять санкции. Это, конечно, приветствуется, но все же такая кажущаяся гибкость должна интерпретироваться очень узко. Предприятия по-прежнему должны соблюдать рекомендации, изданные в связи с выполнением требований по защите данных, а также указания национальных учреждений по надзору за защитой данных в тех странах, где осуществляют свою деятельность.