

Общество с ограниченной ответственностью «Про-потолки»
(ООО «Про-потолки»)

УТВЕРЖДАЮ
Генеральный директор
ООО «Про-потолки»



И.А. Лозука

15.05.2025 года

РЕГЛАМЕНТ

действий на случай утечки персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий регламент (далее — Регламент) разработан с целью незамедлительного реагирования на утечку персональных данных, чтобы минимизировать возможный ущерб.

1.2. В целях Регламента под утечкой персональных данных понимается неправомерное или случайное раскрытие (попадание) персональных данных третьим лицам.

1.3. Регламент является обязательным для всех работников ООО «Про-потолки». Все работники организации должны быть ознакомлены с Регламентом под подпись.

2. ПОРЯДОК ОПОВЕЩЕНИЯ ОБ УТЕЧКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Работник ООО «Про-потолки», которому стало известно о готовящемся или свершившемся инциденте в отношении персональных данных (далее — ПДн), обязан незамедлительно уведомить лицо, ответственное за организацию обработки персональных данных, — специалиста по работе с персональными данными или генерального директора ООО «Про-потолки».

2.1.1. Лицо, ответственное за обработку персональных данных в ООО «Про-потолки», назначается приказом генерального директора.

2.1.2. Телефонный номер, адрес электронной почты и мессенджеры работника, ответственного за обработку ПДн, указаны на корпоративном портале.

2.2. Уведомление об утечке ПДн должно содержать следующую информацию:

- источник получения информации;
- дата и время инцидента с ПДн;
- информация о категориях ПДн (в том числе специальные категории ПДн и биометрические ПДн);
- обстоятельства, в результате которых произошла утечка ПДн;
- информация об информационных системах персональных данных, из которых произошла утечка;
- иные обстоятельства, известные работнику.

3. МЕРЫ РЕАГИРОВАНИЯ НА УТЕЧКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Специалист по работе с персональными данными незамедлительно:

- информирует генерального директора ООО «Про-потолки» о случившемся факте;
- формирует комиссию для реагирования на утечку ПДн и устранения последствий, в которую привлекает системного администратора и специалиста по кадрам;
- инициирует внутреннее расследование;
- координирует и контролирует работу комиссии по реагированию на утечку ПДн.

3.2. Системный администратор:

- блокирует доступ третьих лиц к информационным системам ООО «Про-потолки»;
- определяет, произошла ли утечка ПДн;
- устанавливает причины утечки ПДн;
- устраняет последствия утечки ПДн;
- выявляет лиц, виновных в утечке ПДн;
- предоставляет генеральному директору информацию, необходимую для уведомления Роскомнадзора;
- разрабатывает и внедряет меры для исключения подобных инцидентов в дальнейшем.

3.2.1. Системный администратор в течение 20 часов с момента обнаружения утечки ПДн предоставляет генеральному директору следующую информацию:

- сведения о произошедшем инциденте – дата и время выявления инцидента, характеристики ПДн (содержание базы данных, количество содержащихся в ней записей, актуальность базы данных, период, в течение которого собраны ПДн);
- предварительные причины утечки ПДн;
- предполагаемый вред, нанесенный правам субъектов ПДн, с учетом ранее оформленного акта об оценке возможного вреда субъектам персональных данных;
- принятые меры по устранению последствий соответствующего инцидента – перечень организационных и технических мер по устранению последствий утечки ПДн.

3.2.2. Системный администратор не позднее 65 часов с момента обнаружения утечки ПД предоставляет генеральному директору следующую информацию:

- причины утечки ПДн;
- вред, нанесенный правам субъектов ПДн;
- принятые дополнительные меры по устранению последствий утечки ПДн (при наличии);
- лица, действия которых стали причиной утечки ПДн, – фамилия, имя, отчество, должность работника (если причиной утечки ПДн стали работники ООО «Про-потолки»);
- фамилия, имя, отчество физического лица, индивидуального предпринимателя или полное наименование юридического лица, действия которых стали причиной утечки ПДн, IP-адрес компьютера или устройства, предполагаемое местонахождение таких лиц или устройств, если причиной инцидента стали действия посторонних лиц;
- иные сведения об утечке ПДн.

3.2.3. Если информация из раздела 3.2.2 стала известна системному администратору в течение 20 часов с момента обнаружения утечки ПДн, тогда эту информацию он передает генеральному директору незамедлительно.

3.2.4. Системный администратор имеет право привлекать к решению вопросов по реагированию на утечку ПДн других работников ООО «Про-потолки».

3.3. Специалист по кадрам:

- оценивает вред, нанесенный правам субъектов ПДн;
- совместно с другими членами комиссии выявляет виновных лиц;
- уведомляет Роскомнадзор в случае утечки ПДн.

3.3.1. Специалист по кадрам первичное уведомление в Роскомнадзор направляет не позднее 24 часов с момента обнаружения утечки ПДн.

3.3.2. В первичном уведомлении указывается следующая информация:

- сведения о произошедшем инциденте – дата и время выявления инцидента, характеристики ПДн (содержание базы данных, количество содержащихся в ней записей, актуальность базы данных, период, в течение которого собраны ПДн);
- предварительные причины утечки ПДн;
- предполагаемый вред, нанесенный правам субъектов ПДн;
- принятые меры по устранению последствий соответствующего инцидента – перечень организационных и технических мер по устранению последствий утечки ПДн;
- данные специалиста по работе с персональными данными.

3.3.3. Дополнительное уведомление в Роскомнадзор направляется не позднее 72 часов с момента обнаружения утечки ПДн.

3.3.4. В дополнительном уведомлении указываются реквизиты приказа о проведении внутреннего расследования и результаты внутреннего расследования:

- причины утечки ПДн;
- вред, нанесенный правам субъектов ПДн;
- принятые дополнительные меры по устранению последствий утечки ПДн (при наличии);
- лица, действия которых стали причиной утечки ПДн (при наличии) – фамилия, имя, отчество, должность работника (если причиной утечки ПДн стали работники ООО «Про-потолки»);
- фамилия, имя, отчество физического лица, индивидуального предпринимателя или полное наименование юридического лица, действия которых стали причиной утечки ПДн, IP-адрес компьютера или устройства, предполагаемое местонахождение таких лиц или устройств (если причиной инцидента стали действия посторонних лиц) и иные сведения об утечке ПДн при наличии.

3.3.5. Уведомления направляются в виде документа на бумажном носителе или в форме электронного документа.

3.3.6. Уведомления в виде документа на бумажном носителе направляются по адресу Роскомнадзора.

3.3.7. Уведомления в форме электронного документа направляются посредством заполнения специализированной формы, размещенной на Портале персональных данных Роскомнадзора.

Для этого необходимо пройти аутентификацию на портале госуслуг, заполнить форму и направить ее в электронном виде. При приеме на работу специалист по кадрам оформляет подтвержденную учетную запись на портале госуслуг. Учетную запись привязывают к организации на портале госуслуг.

3.4. Специалист по кадрам:

- оформляет приказ о реагировании на утечку ПДн, создании комиссии и проведении внутреннего расследования;
- оформляет документы на работу в выходной и нерабочий праздничный день для членов комиссии и других работников, которые задействованы в работе по ликвидации последствий утечки ПДн;
- оформляет документы для привлечения к ответственности работников в случае выявления виновных в утечке ПДн.

4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

4.1. Регламент вступает в силу с момента его утверждения.

4.2. Внесение изменений в Регламент производится приказом генерального директора Организации. Изменения вступают в силу с момента подписания соответствующего приказа.