Обязательные корпоративные правила «Roust Group»

Версия: 1.0

Число: 25 мая 2018 г.

Содержание

1. Введение

1. Целью обязательных корпоративных правил («ОКП») является обеспечение адекватной защиты при передаче и обработке персональных данных корпорацией Roust Corporation и ее аффилированными лицами, участвующими в совместной экономической деятельности («Roust Group»).

2. Все компании, входящие в состав Roust Group, выражают свое решительное желание соблюдать ОКП.

3. ОКП налагают на все компании Roust Group и всех сотрудников Roust Group обязательство соблюдать изложенные в ОКП принципы.

2. Термины и определения

В настоящих ОКП используются следующие термины:

1. «Персональные данные» означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу;

   ПРИМЕЧАНИЕ: Идентифицируемое физическое лицо – это лицо, которое можно идентифицировать прямо или косвенно, в частности, посредством таких идентификаторов, как ФИО, идентификационный номер, данные о местоположении, онлайновый идентификатор, а также один или несколько признаков, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица.

2. «Обработка» означает любую операцию или набор операций, выполняемых с персональными данными или наборами персональных данных, с использованием автоматических средств или без использования таковых, например сбор, запись, организация, структурирование, хранение, модификация или изменение, поиск, консультирование, использование, раскрытие посредством передачи, распространение или иное предоставление, упорядочение или комбинирование, ограничение использования, стирание или уничтожение данных;

3. «Контролер» означает субъекта, определяющего цели и средства обработки персональных данных;

4. «Обработчик» означает субъекта, обрабатывающего персональные данные от имени контролера;

5. «Экспортер данных» – это субъект (вне или внутри группы), предоставляющий данные для обработки;

6. «Импортер данных» или «получатель» – это субъект (вне или внутри группы), использующий данные для обработки;

7. «Обязательные корпоративные правила» или «ОКП» – правила обеспечения защиты персональных данных, соблюдаемые контролером или обработчиком;

8. «Член группы ОКП» означает любую компанию, действующую в рамках Roust Group в качестве экспортера или импортера данных, участвующего во внутригрупповой передаче персональных данных из ЕС и в ЕС;

9. «Надзорный орган» означает независимый государственный орган, учрежденный государством-членом ЕС, отвечающий за мониторинг применения ОРЗД (Общего регламента ЕС о защите данных);

10. «Компетентный надзорный орган» означает надзорный орган, учрежденный на территории государства-члена ЕС, которому представляется заявление об ОКП с целью передачи или многократной передачи персональных данных контролеру или обработчику в одной или нескольких третьих странах в рамках группы компаний или группы предприятий, занимающихся совместной экономической деятельностью;

11. «Государство-член» означает страну Европейского союза.

3. Охват и область применения

1. Настоящие ОКП регулируют только передачу и обработку персональных данных, входящих в состав потоков данных, которыми обмениваются члены группы ОКП, учрежденные в ЕС и действующие в рамках Roust Group. Члены группы ОКП перечислены в Приложении «А».

2. Обработка или передача персональных данных, которые осуществляются внутри компаний-членов ОКП, регулируются правилами местной политики, утвержденной руководством данной компании. Такая политика налагает на руководство и сотрудников обязанности по защите персональных данных и санкции за несоблюдение ее правил.

3. ОКП применяются к следующим видам данных, получаемым или предоставляемым в рамках корпоративной деятельности:

- подбор персонала (выше определенного уровня управления);
- управление эффективностью работы сотрудников и их профессиональным развитием;
- расчет заработной платы и администрирование пособиями и выплатами для сотрудников (выше определенного уровня управления);

- корпоративные финансы;
- управление базами данных;
- обучение персонала и представителей подрядчиков;
- управление продажами с использованием данных отдельных лиц (например, подробные ежедневные отчеты о продажах);
- поддержка и развитие отношений с клиентами, включая рассмотрение жалоб и расчеты;
- управление маркетингом с привлечением данных отдельных лиц (например, подробные отчеты о маркетинговых мероприятиях);
- цепочка поставок: авторизация счетов-фактур;
- цепочка поставок: авторизация CAPEX (капитальных затрат);
- предупреждения об опасности в области охраны труда и промышленной безопасности;
- информация, необходимая для предотвращения или расследования мошенничества или других целей, связанных с системой управления рисками.

Описание потоков данных между странами представлено в Приложении «Б».

4. Кроме того, персональные данные обрабатываются горизонтально всеми членами группы ОКП с целью управления идентификацией сотрудников и представителей подрядчиков, а также с целью проверки информации в ИТ-системах компании Roust Group (например, Helpdesk).

4. Права субъекта данных

1. Все члены группы ОКП предпринимают меры по соблюдению основных прав любого субъекта данных, а именно:

    a. Личные данные передаются и обрабатываются в конкретных, законных и не чрезмерных целях. Субъекту данных предоставляется ясная и исчерпывающая информация (обычно в форме заявления о добросовестной обработке данных) о способе использования и раскрытии данных (в том числе вторичном использовании и раскрытии данных), получателях или категориях получателей персональных данных и личности контролера данных, если такие данные были получены членом группы ОКП.

    b. Персональные данные должны быть точными и актуальными. Каждый член группы ОКП активно рекомендует субъектам данных сообщать соответствующему контролеру данных об изменении своих персональных данных.

    c. Персональные данные хранятся столько, сколько это необходимо. Персональные данные всегда хранятся и/или удаляются в объеме, предусмотренном законом,

нормативными актами и профессиональными стандартами, в соответствии с применимой к данному случаю политикой хранения данных члена группы ОКП. По истечении срока хранения данных член группы ОКП удаляет персональные данные только безопасным способом в соответствии с местной политикой безопасности.

d. Персональные данные собираются и обрабатываются в минимальном объеме, необходимом для достижения целей обработки.

e. Уязвимые данные[1] используются только тогда, когда это абсолютно необходимо. В таком случае доступ к конфиденциальным персональным данным ограничен определенным кругом лиц (путем сокрытия или обезличивания данных в соответствующих случаях).

f. Персональные данные не передаются внешним третьим лицам без обеспечения адекватной защиты данных.

2. Субъекту данных предоставляется право доступа, исправления, стирания, ограничения данных и возражения против их обработки. Вышеуказанные права не должны обеспечиваться механизмами, основанным исключительно на автоматизированной обработке, включая профилирование. Процедура предоставления доступа к данным описана в приложении «В».

3. Субъект данных вправе подать жалобу в соответствии с внутренней процедурой каждого члена группы ОКП. Кроме того, субъект данных может подать жалобу в компетентный надзорный орган по своему месту проживания, месту работы или месту предполагаемого нарушения либо в суд государства-члена ЕС по своему выбору. Процедура рассмотрения жалоб подробно описана в Приложении «Г».

4. В случае потенциального или фактического нарушения персональных данных соответствующий член группы ОКП обязан соблюдать процедуру, указанную в Приложении «Д» настоящего документа, и сотрудничать в наибольшей возможной степени с соответствующим надзорным органом.

5. Субъекту данных предоставляется право на судебные средства правовой защиты, получение возмещения ущерба и, при необходимости, компенсацию в случае нарушения ОКП, как указано выше в подпункте 1 (a-f) пункта 4.

[1] Уязвимые данные – это данные, относящиеся к расовому или этническому происхождению человека, политическим взглядам, религиозным или иным убеждениям, членству в профсоюзах, состоянию здоровья, половой жизни, судимости, социальному обеспечению, государственным идентификационным номерам или номерам финансовых счетов.

5. Прозрачность и право на информацию

1. До начала обработки данных субъектам данных предоставляется следующая информация:
    a. сведения, идентифицирующие контролера и его представителя (при его наличии);
    b. предполагаемые цели обработки данных;
    c. дополнительная информация, например:
    i) о получателях или категориях получателей данных,
    ii) о наличии права на доступ к данным, относящимся исключительно к данному субъекту данных, и их исправление,
    iii) об условиях предоставления возможности, по запросу субъекта данных, прекратить и заблокировать обработку данных, в том числе при необходимости удалить данные,
    iv) о предусмотренных законом процедурах обработки (как для субъектов данных, чьи данные собираются напрямую, так и посторонних бенефициаров, например, клиентов экспортера данных).

2. Каждый субъект данных имеет право получить беспрепятственный доступ к своим данным.
3. Каждый член группы ОКП собирает, передает и обрабатывает персональные данные только в ясно сформулированных и законных целях, указанных в ОКП. Если персональные данные были получены от третьих лиц (включая клиентов членов группы ОКП) и из общедоступных источников, следует всегда использовать надежные и авторитетные источники.
4. Член группы ОКП передает персональные данные только в случае, если:
    a. соблюдаются все применимые требования законодательства;
    b. передача осуществляется в связи с четко выраженной деловой необходимостью;
    c. импортер данных внедрил соответствующие меры безопасности.
5. Члену группы ОКП нельзя раскрывать персональные данные за исключением случаев, указанных в ОКП, его политике или в случаях, когда это требуется или иным образом допускается на основании договоров или применимого законодательства.

6. Организация защиты данных

1. Директор по вопросам безопасности и нормативно-правового соответствия в CEDC International sp. z o.o. (член группы ОКП в Польше) назначается главным инспектором по защите данных («Главный ИЗД»).

2. К задачам Главного ИЗД относятся:

    a. общий надзор за выполнением ОКП;

    b. консультирование и поддержка совета директоров Roust Corporation в отношении всех аспектов ОКП;

    c. мониторинг соблюдения правил на корпоративном уровне и соответствующая отчетность;

    d. поддержка местных ИЗД и сотрудничество в случае инцидентов, связанных со сферой применения ОКП;

    e. участие в расследованиях, проводимых надзорными органами;

3. Главный ИЗД подчиняется непосредственно совету директоров Roust Corporation.

4. Член группы ОКП может назначить своего местного инспектора по защите данных («ИЗД»). Если последний не был назначен, обязанности инспектора по защите данных принимает на себя назначенный менеджер. Список назначенных лиц в каждой стране ведет Главный ИЗД.

5. К задачам ИЗД относятся:

    a. мониторинг защиты, обработки и передачи данных в рамках ОКП на местном уровне;

    b. проведение аудитов в соответствии с программой аудита ОКП;

    c. рассмотрение местных жалоб от субъектов данных в рамках ОКП;

    d. принятие мер в случае инцидентов, связанных со сферой применения ОКП на местном уровне, и в соответствующих случаях сотрудничество с другими ИЗД и Главным ИЗД;

    e. передача Главному ИЗД сообщений о серьезных проблемах, связанных с конфиденциальностью данных;

    f. организация и мониторинг тренингов на местном уровне;

g. оказание соответствующему надзорному органу помощи в проведении аудита или расследования, а также внедрение советов и рекомендаций надзорного органа.

7. Меры безопасности и их эффективность

1. Член группы ОКП использует соответствующие технические, организационные, административные и физические меры безопасности для защиты персональных данных от несанкционированной или незаконной обработки, случайной потери или уничтожения.

2. Каждая трансграничная передача персональных данных между членами группы ОКП защищается при помощи соответствующих криптографических методов, обеспечивающих конфиденциальность данных.

3. В обмене персональными данными между членами группы ОКП могут участвовать только надлежащим образом уполномоченные сотрудники.

4. Ответственность за мониторинг, регулярный пересмотр и совершенствование системы безопасности, политики и процедур с учетом возникающих угроз, а также за новые технологические меры безопасности и предосторожности несут соответствующие ИТ-отделы.

5. Когда член группы ОКП поручает обработку персональных данных третьему лицу, данный член ОКП должен выбрать надежных третьих лиц, которые внедрили соответствующие меры безопасности. В частности, третье лицо обязано незамедлительно уведомлять члена группы ОКП ЕС, соответствующего инспектора по защите данных и субъектов данных обо всех нарушениях персональных данных, если нарушение персональных данных может повлечь за собой серьезную угрозу их правам и свободам.

6. Любые нарушения безопасности персональных данных, связанные с ОКП (т. е. факты, связанные с нарушением безопасности персональных данных, последствия нарушения и меры по исправлению положения) документируются, а документация предоставляется надзорному органу.

7. Сотрудники, имеющие постоянный или регулярный доступ к персональным данным и участвующие в сборе данных или разработке инструментов, используемых для обработки персональных данных, проходят соответствующее обучение в сфере ОКП.

8. Все аспекты ОКП, в том числе методы, обеспечивающие выполнение корректирующих действий, подлежат регулярному аудиту.

9. Общая программа аудита ОКП разрабатывается Главным инспектором по защите персональных данных и выполняется по согласовании с советом директоров Roust Corporation.

10. Результаты всех аудитов доводятся до сведения Главного инспектора по защите персональных данных.

11. Главный инспектор по защите персональных данных или соответствующий местный инспектор по защите данных обеспечивает доступ соответствующих надзорных органов к результатам аудита по их запросу и по мере необходимости помогает надзорному органу при проведении аудита защиты данных у любого члена группы ОКП.

8. Подотчетность и соблюдение закона

1. Каждый член ОКП, выполняющий функцию контролера данных, несет ответственность за соблюдение ОКП и должен быть в состоянии доказать их соблюдение.

2. Чтобы доказать соблюдение ОКП, члены группы ОКП ведут учет всех видов деятельности по обработке данных, осуществляемых в соответствии с требованиями, изложенными в ОРЗД. Учетные документы предоставляется по запросу соответствующему надзорному органу.

3. Для обеспечения соблюдения основных принципов защиты данных вводятся соответствующие технические и организационные меры, т. е. встроенный алгоритм конфиденциальности и конфиденциальность по умолчанию.

4. Оценка воздействия на защиту данных проводится, если выполняются соответствующие критерии, предусмотренные ОРЗД.

9. Применимое право и ответственность

1. ОКП соответствуют соответствующему законодательству ЕС, в частности, Общему регламенту по защите данных («ОРЗД»), и местному законодательству в соответствующих странах, в которых осуществляют деятельность компании группы Roust Group.

– Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене директивы 95/46/ЕС (Общий регламент ЕС о защите данных, «ОРЗД»);

- Закон о конфиденциальности [Privacy Act] (R.S.C., 1985, c. P-21) (Канада);
- Закон о защите личной информации и электронных документах [PIPEDA] (Канада);
- Проект закона, вносящего изменения в венгерское законодательство о защите данных (Венгрия);
- Проект закона о защите персональных данных (Польша);
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Россия);
- Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» (с изменениями и дополнениями) (Россия);
- Закон о защите персональных данных (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481) (Украина);
- Указ об утверждении документов в области защиты персональных данных, Наказ 08.01.2014 № 1 / 02-14 (Украина).

2. Если местное законодательство требует более высокого уровня защиты персональных данных, оно будет иметь приоритет над ОКП.

3. Каждый член группы ОКП в ЕС, экспортирующий данные из ЕС на основании ОКП, несет ответственность за нарушения ОКП членом ОКП с местом нахождения за пределами ЕС, получившим данные от этого члена группы ОКП.

4. Несущий ответственность член группы ОКП вправе доказать, что член группы ОКП за пределами ЕС не виновен в нарушении правил, в связи с которым субъект данных требует возмещения ущерба. В таком случае член группы ОКП освобождается от какой-либо ответственности.

10. Исключения из соблюдения ОКП

1. В случае, когда у члена группы ОКП есть основания полагать, что применимое к нему законодательство не позволяет компании выполнять вытекающие из ОКП обязательства или существенным образом влияет на гарантии, предусмотренные этими правилами, такой член незамедлительно информирует об этом Главного инспектора по защите персональных данных и соответствующего инспектора по защите данных, за исключением случаев, когда это запрещено правоохранительным органом, например, в соответствии с уголовным законодательством с целью сохранения конфиденциальности при расследовании дела правоохранительным органом.

2. Кроме того, если требование законодательства, применимого к члену группы ОКП в третьей стране, может оказать существенное

негативное влияние на изложенные в ОКП гарантии, о данной проблеме следует сообщить в соответствующий надзорный орган. Это касается юридически обязывающего запроса правоохранительного органа или органа государственной безопасности о раскрытии персональных данных. В таком случае надзорному органу должна быть передана четкая информация о запросе, в том числе информация о запрошенных данных, запрашивающем органе и правовой основе раскрытия информации (например, запрет на сохранение конфиденциальности данных в случае расследования на основании уголовного законодательства).

3. Если в определенных случаях приостановка или уведомление запрещены законом, то соответствующий член группы ОКП должен приложить все усилия для получения права не соблюдать такой запрет, чтобы передать как можно больше информации в кратчайшие сроки и доказать, что это было сделано.

4. Если во всех вышеперечисленных случаях член группы ОКП не в состоянии уведомить соответствующий надзорный орган, он обязан ежегодно предоставлять общую информацию по запросу надзорного органа (например, по возможности, информацию о числе запросов о раскрытии данных, виде запрашиваемых данных, запрашивающем лице).

5. В любом случае передача персональных данных членом группы ОКП государственным органам не может быть масштабной, непропорциональной, бесконтрольной и выходить за рамки того, что необходимо в демократическом обществе.

11. Актуализация ОКП

1. ОКП актуализируются при наличии хотя бы одного из следующих условий:

– существует необходимость внести какие-либо значительные изменения в текст ОКП,

– изменилась нормативная база в сфере прав и обязанностей надзорных органов,

– произошли изменения в структуре компании или корпорации, в результате которых требуются новые полномочия / утверждение надзорного органа.

2. Если изменения могут повлиять на гарантируемый ОКП уровень защиты или существенным образом повлиять на характер ОКП (т. е. повлечь изменение их обязательного статуса), такая информация должна быть незамедлительно передана соответствующим надзорным органам через компетентный надзорный орган.

3. После утверждения изменений советом директоров Roust Corporation Главный инспектор по защите персональных данных обязан сообщить об изменениях без неоправданной задержки всем членам группы ОКП и соответствующим надзорным органам через компетентный надзорный орган.

4. Следующие изменения ОКП не нуждаются в повторном утверждении компетентным надзорным органом:

- Главный инспектор по защите персональных данных ведет регулярно актуализируемый список членов группы ОКП, отслеживает и фиксирует все актуализации правил и предоставляет субъектам данных или надзорным органам необходимую информацию по их запросу;

- новому члену ОКП не передаются данные до тех пор, пока он не примет ОКП и не сможет доказать их соблюдение;

- раз в год соответствующий надзорный орган уведомляется через компетентный надзорный орган об изменениях ОКП или списка членов ОКП с кратким изложением причин актуализации.

Приложение «А» – Список членов группы ОКП

Roust Corporation	CEDC International sp. z o.o
232 Madison Avenue, Suite 1600, NY 10016 New York, USA	ul. Kowanowska 48, 64-600 Oborniki, Poland
PWW sp. z o. o.	B2B Wine &Spirits sp. z o.o.
ul. Bobrowiecka 8, 00-728 Warszawa, Poland	Lubińska 10, 05-532 Lubna, Poland
ROUST Hungary Kft.	ROUST UKRAINE LLC
Alkotás u. 50 1123 Budapest, Hungary	Konstantinovskaya str, 2A, 04071, Kiev, Ukraine
JSC «Roust Russia»	“Parliament Production”, LLC
Eniseiskaya str., b. 1, con.1, 129344, Moscow, Russian Federation	Balashiha, microregion Saltikovka, Popovka str., ownership 5, 143916, Moscow region, Russian Federation
“Russian Standard Vodka” LLC	Bravo Premium LLC
Pulkovskoe shosse 46, build 2, 196140, Saint-Petersbourg, Russian Federation	Kuznetsovskaya str., b. 52, con.3, letter A, 196105, Saint-Petersbourg, Russian Federation
CJSC “ROUST INC.”	Roust Distribution Limited
Shoushari village, Pulkovskoe road, b.52, letter A, 196140, Saint-Petersbourg, Russian Federation	Diagorou 4, Kermia, Building, 6th floor, Office 601, Nicosia, P.C. 1097, Cyprus
Roust Distribution (UK establishment of ROUST DISTRIBUTION LIMITED)	Russian Standard Vodka (USA), Inc.
Thomas House, 84 Eccleston Square, London, United Kingdom, SW1V 1PX	c/o Corporation Service Company, 2711 Centerville Road, Suite 400, in the City of Wilmington, County of New Castle, Delaware, USA
JOINT STOCK COMPANY "DISTILLERY TOPAZ"	“Trading House “Russian Alcohol – Moscow” LLC
46, Oktyabrskaya str., Pushkin, Moscow region, 141200, Russian Federation	1/1, Eniseyskaya str., Moscow, 129344, Russian Federation
Russian Standard Vodka Canada Ltd.	F.lli Gancia & c. spa
Suite 4000, Bay street, 199, Toronto, Ontario, Canada, M5L 1A9	Corso liberta 66, 14053 Canelli, Asti, Italy

Приложение «Б» – Описание потоков данных

Потоки данных в рамках соответствующего трансграничного обмена между членами группы ОКП (для отдельных стран)

Типы данных, **передаваемых** или **сообщаемых** в головной офис или подлежащих внутригрупповому обмену*, в рамках который **могут** появляться персональные данные	Компании в отдельных странах							Замечания по странам
	Россия	Польша	Украина	Велико-британия/ Кипр	США/Канада	Венгрия	Италия	
Подбор персонала – выше определенного уровня управления	нет	да	да	да	да	да	нет	
Управление эффективностью работы сотрудников и их профессиональным развитием;	нет	нет	да	нет	да	да	да	
Расчет заработной платы и администрирование пособиями и выплатами для сотрудников - выше определенного уровня управления;	да	да	да	да	да	да	да	
Корпоративные финансы;	да	да	да	нет	да	да	да	
Управление базами данных;	нет	нет	нет	да	неприм.	да	да	Венгрия: владельцем венгерского юридического лица является CEDC, поэтому те и другие похожие данные могут передаваться в CEDC
Обучение персонала и представителей подрядчиков;	нет	нет	да	нет	нет	нет	нет	
Управление продажами с использованием данных отдельных лиц (например, подробные ежедневные отчеты о продажах);	нет	да	да	нет	нет	нет	нет	Венгрия: такие данные сообщаются, но не указываются данные на уровне конкретных отдельных сотрудников отдела продаж
Поддержка и развитие отношений с клиентами, включая рассмотрение жалоб и финансовые расчеты;	нет	нет	да	нет	неприм.	нет	нет	
Управление маркетингом с привлечением данных отдельных лиц (например, подробные отчеты о маркетинговых мероприятиях);	неприм.	нет	нет	нет	да	нет	нет	США: для моделей промо-акций, имена и фамилии появляются на счет-фактурах
Цепочка поставок: авторизация счетов-фактур;	нет	да	да	нет	нет	нет	неприм.	
Цепочка поставок: авторизация CAPEX (капитальных затрат);	нет	да	да	нет	нет	да	нет	
Предупреждения об опасности в области охраны труда и промышленной безопасности;	нет	да	да	неприм.	неприм.	нет	неприм.	
Информация, необходимая для предотвращения или расследования мошенничества или других целей связанных с системой управления рисками;	нет	нет	да	нет	да	нет	нет	США: информация была предоставлена аудитору при расследовании мошенничества с кредитными картами
Идентификация (управление идентификацией сотрудников и представителей подрядчиков), а также проверка информации (например, Helpdesk);	да	да	да	нет	да	да	да	
*между всеми или некоторыми компаниями Roust Corporation								

Ответ	**Значение**
да	отчеты могут содержать персональные данные (например, данные сотрудников или клиентов)
нет	отчеты имеют агрегированный характер и не содержат персональные данные
неприменимо	такой тип данных не подлежит обработке в данной компании

Приложение «B» – Процедура запроса субъекта данных о предоставлении доступа к его данным

Введение

Законодательство ЕС о защите данных предоставляет лицам, чьи персональные данные собираются и/или передаются на территории ЕС, право на получение информации о том, что их персональные данные обрабатываются данной организацией. Согласно ст. 15 Общего регламента ЕС о защите персональных данных (ОРЗД), субъект данных имеет право на доступ к следующей информации:

(a) цели обработки данных;

(b) категории обрабатываемых данных;

(c) получатели или категории получателей, которым были или будут переданы персональные данные, в частности, получатели данных в третьих странах или международные организации;

(d) по мере возможности, предусмотренный срок, в течение которого будут храниться персональные данные, или, если его невозможно определить, – критерии, используемые для определения этого срока;

(e) наличие у него права требования от контролера исправления или удаления его персональных данных, ограничения их обработки или возражения против такой обработки;

(f) право подачи жалобы в надзорный орган;

(g) если персональные данные получены не от субъекта данных – право на получение доступной информации об источнике данных;

(h) наличие автоматизированной процедуры принятия решений, в том числе профилирования, и право на получение в таких случаях достоверной информации о логической схеме профилирования, а также о важности и предполагаемых последствиях такой обработки для субъекта данных.

Кроме того, если персональные данные передаются в третью страну или международную организацию, субъект данных имеет право получить информацию о предпринимаемых мерах обеспечения безопасности.

Все субъекты данных, чьи персональные данные собираются и используются на территории ЕС **и, кроме того**, передаются между членами группы ОКП, имеют право на доступ к своим данным в соответствии с условиями настоящей процедуры. Если применимое законодательство о защите данных вне ЕС отличается от какого-либо аспекта настоящей процедуры, преимущественную силу имеет данное местное законодательство о защите данных.

Общие положения

1. Запрос направляется в письменной форме, в частности, он может быть направлен по электронной почте.

2. Процедура касается запроса субъекта данных о предоставлении доступа к данным в связи с ОКП (обоснованный запрос).
3. Член группы ОКП не обязан удовлетворять запрос, если субъект данных, подавший запрос, не предоставил достаточную информацию для подтверждения своей личности.
4. Член группы ОКП должен ответить на обоснованный запрос в течение 30 календарных дней с момента получения запроса (или в более короткий срок, который может быть предусмотрен местным законодательством).
5. При нормальных обстоятельствах за удовлетворение запроса не взимается плата, но решение оставляется на усмотрение члена группы ОКП, принявшего запрос, действующего в соответствии с местным применимым законодательством.

Получение и принятие запроса к рассмотрению

6. Если какой-либо сотрудник, партнер или подрядчик члена группы ОКП получает от физического лица запрос о предоставлении доступа к персональным данным, такой запрос немедленно передается соответствующему местному ИЗД (инспектору по защите персональных данных) вместе с датой получения и любой другой информацией, которая может помочь ИЗД в рассмотрении запроса.
7. Местный ИЗД проводит предварительную оценку запроса для установления его обоснованности.
8. Местный ИЗД связывается с подавшим запрос физическим лицом в письменной форме и предпринимает как минимум один из нижеуказанных шагов:
    a. подтверждает принятие запроса к дальнейшему рассмотрению,
    b. запрашивает дополнительную информацию, в частности, для подтверждения личности,
    c. отклоняет запрос в связи с его необоснованностью.
9. Запрос может быть отклонен (п. 8 «c») по следующим основаниям (одному или нескольким):
    a. Если запрос был направлен члену группы ОКП и связан с использованием или сбором персональных данных этим членом группы ОКП, а отказ предоставить информацию основан на законодательстве о защите данных, применяемом на данной юрисдикционной территории;
    b. Если по мнению члена группы ОКП:
        i. выполнение запроса может нанести ущерб основным деловым интересам члена группы ОКП (в том числе в связи с управленческим планированием, корпоративными финансами или переговорами с подавшим запрос субъектом);

ii. отказ необходим по причинам, связанным с государственной или общественной безопасностью, обороной или деятельностью государства в области уголовного права;

iii. отказ необходим для защиты самого субъекта данных или прав и свобод других лиц;

c. Если персональные данные хранятся членом группы ОКП в неавтоматизированной форме, не являются и не станут частью системы хранения документов;

d. Если для предоставления персональных данных член группы ОКП должен приложить непропорционально большие усилия.

10. Местный ИЗД может направлять сложные случаи главному ИЗД для консультаций, особенно в тех случаях, когда в запросе имеется информация, относящаяся к третьим лицам, или когда раскрытие персональных данных может нанести ущерб коммерческой тайне или судебному разбирательству.

Поиск и ответ

11. Местный ИЗД организует поиск во всех соответствующих электронных и бумажных системах хранения документов.

12. Запрошенная информация преобразуется местным ИЗД в понятный формат (например, до передачи данных субъекту удаляются внутренние коды или идентификационные номера, присвоенные персональным данным). Затем местный ИЗД передает субъекту данных всю информацию, необходимую для удовлетворения запроса.

13. Если предоставление информации в форме отдельного документа невозможно или если это потребует непропорциональных усилий, нет обязанности предоставлять информацию в форме отдельного документа. В таких случаях может быть предоставлена возможность доступа к информации путем проверки данных, удаленного доступа к базе данных или получения информации в другой форме.

Просьбы об удалении, исправлении или прекращении обработки информации

14. Если поступил запрос об удалении персональных данных физического лица, он должен быть рассмотрен и должным образом удовлетворен местным ИЗД. Если обработка данных осуществляется в связи с другими важными и легальными основаниями, запрос отклоняется.

15. Если поступил запрос об изменении персональных данных физического лица, данные должны быть соответствующим образом исправлены или актуализированы, если для этого существуют законные основания.

16. Если поступил запрос о прекращении обработки персональных

данных физического лица в связи с тем, что в результате такой обработки, проводимой членом группы ОКП, ущемляются права и свободы человека, местный ИЗД должен передать данный запрос главному ИЗД для дальнейшего рассмотрения. Если проводимая членом группы ОКП обработка является необходимой на каком-либо законном основании, запрос отклоняется.

Приложение «Г» – Процедура рассмотрения жалоб

Введение

Если субъект данных считает, что его персональные данные были обработаны с нарушением ОКП, он может сообщить о своих сомнениях любому члену группы ОКП в письменной форме, по электронной почте или другими способами, указанными в ОКП, с использованием контактных данных, приведенных в Приложении «А» к ОКП.

Целью данной процедуры является разъяснение способа рассмотрения жалоб, поданных лицами, чьи персональные данные обрабатываются членом группы ОКП и в рамках группы ОКП.

Рассмотрение жалобы

1. Если какой-либо сотрудник, партнер или подрядчик члена группы ОКП получает жалобу относительно ОКП, такую жалобу следует немедленно передать соответствующему местному ИЗД вместе с датой получения и любой другой информацией, которая может помочь ИЗД в ее рассмотрении.
2. Местный ИЗД подтверждает получение жалобы соответствующему лицу в течение 5 рабочих дней.
3. Местный ИЗД рассматривает жалобу при поддержке соответствующих деловых или других организационных подразделений, а также, в случае необходимости, при поддержке главного ИЗД.
4. В обычных условиях местный ИЗД подготавливает ответ подавшему жалобу лицу в течение 30 дней. При невозможности ответить в указанный срок из-за сложности жалобы местный ИЗД информирует об этом данное лицо с указанием предполагаемого срока предоставления ответа. В любом случае этот срок не может превышать шести месяцев с даты подачи жалобы.

Разрешение споров

5. Если заявитель жалобы ставит под сомнение ответ или какой-либо аспект выводов, сделанных местным ИЗД, данный вопрос передается главному ИЗД, который рассматривает дело и принимает решение об оставлении исходного ответа в силе или о его изменении.
6. Главный ИЗД принимает все разумные меры для разрешения спора.
7. Действия главного ИЗД не могут продолжаться дольше 60 дней с даты повторной подачи жалобы.

Заключительные положения

Независимо от описанной выше процедуры лицо, чьи персональные данные собираются и/или используются, имеет право подать жалобу в единый надзорный орган, в частности, в государстве-члене ЕС, в котором оно

проживает или работает, а также право на рассмотрение спора в судебном порядке в соответствии с положениями ОРЗД, в частности, если данное лицо не удовлетворено результатами рассмотрения его жалобы, относящейся к ОКП.

Лица, имеющие такие права, будут уведомлены об этом соответствующим образом в рамках процедуры рассмотрения жалоб.

Приложение «Д» – Процедура, применяемая в случае инцидентов

Введение

Нарушение безопасности персональных данных (в дальнейшем – «инцидент») может произойти по ряду причин, например:

- потеря или кража данных или оборудования, на котором хранятся данные, или посредством которых можно получить доступ к данным;
- потеря или кража бумажных документов;
- несанкционированный доступ к данным (например, в результате хакерской атаки);
- неадекватный контроль доступа, допускающий несанкционированный / необоснованный доступ к данным;
- неисправность оборудования;
- ошибка администратора или пользователя;
- непредвиденные обстоятельства, такие как пожар или наводнение.

Общий регламент ЕС о защите персональных данных гласит, что как только контролеру (в рамках ОКП – соответствующего члена группы ОКП) станет известно, что произошло нарушение безопасности персональных данных, о таком инциденте следует без неоправданной задержки оповестить соответствующий надзорный орган, по возможности, не позднее чем в течение 72 часов после подтверждения информации об инциденте, кроме случаев, когда член группы ОКП ЕС сможет доказать, в соответствии с принципом подотчетности, что нарушение безопасности персональных данных, по всей вероятности, не приведет к появлению угрозы для прав и свобод физических лиц.

Сообщение об инциденте

1. Если обнаружено или есть подозрения, что произошло нарушение безопасности персональных данных, об инциденте следует немедленно сообщить местному ИЗД.
2. Для выявления угроз безопасности персональных данных и их устранения до возникновения нарушений любой сотрудник, партнер или подрядчик должен сообщать о ситуациях, близких к промаху (т. е. инцидентах, которые почти привели к утечке персональных данных, но ее удалось предотвратить благодаря быстрому вмешательству или просто удачному стечению обстоятельств).

Расследование инцидента

3. Первую оценку инцидента проводит местный ИЗД.
4. Если инцидент влияет на трансграничный обмен персональными данными, тогда местный ИЗД без неоправданной задержки сообщает об этом должностным лицам из соответствующих членов группы

ОКП и главному ИЗД. Работу команд инспекторов по защите данных координирует местный ИЗД, в чьем ведении находится соответствующий член группы ОКП ЕС, или главный ИЗД, если это уместно.

5. Команда инспекторов по защите данных из соответствующих членов группы ОКП дополнительно анализирует данный случай и принимает решение о необходимости принятия неотложных мер, направленных на изменение, ограничение или расширение действий в данной ситуации.
6. В зависимости от типа и серьезности инцидента, а также по решению команды инспекторов по защите данных, представляющих соответствующих членов группы ОКП, местный ИЗД или главный ИЗД (т. е. лицо, назначенное координатором команды):
    - актуализирует журнал нарушений безопасности персональных данных и закрывает журнал, если инцидент не требует дополнительных оценок; или
    - открывает расследование и назначает соответствующую следственную группу, состоящую из внутренних или внешних экспертов (например, представляющих ИТ-подразделение соответствующих членов группы ОКП);
    - осуществляет мониторинг деятельности следственной группы и проводит текущую оценку инцидента.
7. Следствие должно принести следующие результаты:
    - определение характера и масштаба инцидента, вида и объема данных, а также идентификация субъектов данных;
    - оценка риска с точки зрения прав и свобод субъектов данных;
    - указание действий, которые должны предпринять члены группы ОКП, чтобы приостановить нарушение и восстановить информацию;
    - рекомендация действий, необходимых для предотвращения повторения инцидента в будущем.
8. В случае, если текущие оценки показывают, что инцидент нельзя своевременно купировать, сообщение об этом передается главному ИЗД и руководству заинтересованных членов группы ОКП ЕС.
9. На основании результатов расследования местный ИЗД или главный ИЗД (если это уместно) готовит полный ретроспективный (ex-post) отчет о нарушениях и актуализирует журнал нарушений безопасности персональных данных.

Сообщение о нарушении в соответствующий надзорный орган или субъектам данных

10. Если было доказано, что появилась серьезная угроза для прав и свобод субъектов данных, местный ИЗД из соответствующей компании-члена группы ОКП ЕС или главный ИЗД (если это уместно)

координирует процедуру передачи отчета об инциденте в соответствующий надзорный орган. Информацию об инциденте получает также правление заинтересованной компании-члена группы ОКП или, в случае необходимости, члены корпоративного управления.

11. Кроме того, если имело место нарушение, информация об инциденте без неоправданной задержки сообщается субъектам данных. Такую информационную кампанию координирует местный ИЗД из соответствующей компании-члена ОКП ЕС или главный ИЗД (если это уместно), при поддержке соответствующих юридических служб и/или PR-подразделений.

Действия, предпринимаемые после инцидента

После закрытия инцидента главный ИЗД проверяет журнал нарушений безопасности персональных данных или ретроспективный отчет о нарушении, чтобы оценить необходимость внесения изменений в ОКП. Главный ИЗД координирует процесс обучения и передачу информации, подготовленной на основании сделанных выводов.