ВСЕМИРНЫЙ ПОЧТОВЫЙ СОЮЗ

Приложение 1 к письму 3911(DPRM.PPRE.PRA)1159
от 5 декабря 2023 г.

Обзор нормативно-правовой базы стран-членов в области сбора и защиты данных в международном почтовом обмене

Назначенным операторам стран-участниц настоятельно рекомендуется вернуть эту форму (без сопроводительного письма) как можно скорее, **но не позднее 19 января 2023 года**, по следующему адресу:

Bonseung Ku
Associate Expert, Policy and Regulatory Advisory
International Bureau
Weltpoststrasse 4
Case postale
3000 BERNE 15
SWITZERLAND

Также можно вернуть заполненную анкету на э-адрес bonseung.ku@upu.int

При возникновении проблем в заполнении анкеты обращайтесь г-ну Бонсеунгу Ку в Международном бюро (+41 31 350 35 24 или bonseung.ku@upu.int).

Пожалуйста, опишите тип вашей организации (выберите один) ❑ Министерство по надзору (ответственное за почтовый сектор) ❑ Регулирующий орган (ответственный за почтовый сектор) ❑ Назначенный оператор	
Название организации	
ФИО ❑ Г-н ❑ Г-жа	
Должность	
Адрес	
Страна	
Тел.	Факс

Вопросник

Часть I – Общие вопросы

1. Каким правилам защиты данных/конфиденциальности[1] вы подчиняетесь при осуществлении почтовых операций в вашей стране?

   ❑ Общий регламент защиты данных (GDPR) (Регламент Европейского союза)

   ❑ Федеральный закон Швейцарии о защите данных (FADP)

   ❑ Закон Калифорнии о защите прав потребителей (CCPA)

   ❑ Общий закон Бразилии о защите персональных данных (LGPD)

   ❑ Нет

   ❑ Прочее (просьба указать):

2. Существуют ли в вашей стране специальные правила[2] защиты данных для почтового сектора?

   ❑ Да (просьба указать):

   ❑ Нет

3. Существуют ли другие межсекторальные правила защиты данных, например, в отношении таможни и транспорта, которые имеют отношение к почтовому сектору в вашей стране?

   ❑ Да (просьба указать):

   ❑ Нет

4. Для каких целей вы собираете персональные данные[3] и обмениваетесь ими с другими сторонами при работе международных почтовых служб? Пожалуйста, выберите все применимые варианты (возможно более одного ответа):

   ❑ Оперативные цели (сбор, обработка, отслеживание/идентификация отправления, адресация, доставка и т.д.)

   ❑ Таможня и безопасность (предварительные электронные данные, данные ITMATT и т.д.)

   ❑ Качество услуг (например, отзывы клиентов и эффективность доставки)

   ❑ Финансовая и бухгалтерская информация (например, информация о выставлении счетов, платежные реквизиты)

   ❑ Прочее (просьба указать):

[1] Правила защиты данных/конфиденциальности относятся к правилам и стандартам, которые регулируют сбор, использование, хранение и общий доступ к персональным данным.
[2] Специальные правила для сектора – это те, которые применяются только к почтовому сектору и могут содержать иные или дополнительные требования, чем общие правила защиты данных.
[3] Персональные данные относятся к любой информации, которая может быть использована для идентификации физического лица или установления его связи с ним.

Многостороннее соглашение ВПС об обмене данными (MDSA), принятое СПЭ в апреле 2021 года, является правовым документом, созданным для облегчения обмена данными, необходимыми для функционирования международных почтовых служб, и обеспечения возможности осуществления таких обменов в соответствии с Актами ВПС.

MDSA включает в себя и расширяет основные положения существующих и созданных в частном порядке многосторонних соглашений об обмене данными, заключенных назначенными операторами стран-членов Союза. Цель состоит в том, чтобы лучше отразить соответствующие обязательства по обмену данными, содержащиеся в Актах Союза, и создать соответствующие условия для управляемого ВПС инструмента с глобальным охватом.

5. Являетесь ли вы участником MDSA ВПС?

- ❑ Да
- ❑ Нет
- ❑ Прочее (просьба указать):

Часть II – Подотчетность

6. Есть ли у вас специальный сотрудник по защите данных (DPO) или аналогичное лицо, ответственное за обеспечение соблюдения обязательств по защите данных и конфиденциальности? (Пожалуйста, выберите только один ответ из следующих):

- ❑ У нас есть специальный DPO или команда, которые регулярно отслеживают и обновляют нашу политику и процедуры
- ❑ Мы полагаемся на внешних консультантов или аудиторов, которые периодически проверяют и консультируют нас по нашей политике и процедурам
- ❑ У нас нет официального DPO или команды, которые регулярно отслеживают и обновляют нашу политику и процедуры
- ❑ Прочее (просьба указать):

7. Как вы демонстрируете подотчетность за защиту данных/конфиденциальность перед своими клиентами и партнерами? Пожалуйста, выберите все применимые варианты (возможно более одного ответа):

- ❑ Мы публикуем нашу политику конфиденциальности данных и уведомления на нашем веб - сайте и по другим каналам связи
- ❑ Мы проводим регулярные оценки воздействия на защиту данных[4] и аудиты и сообщаем о их результатах нашим заинтересованным сторонам
- ❑ У нас нет конкретного способа продемонстрировать нашу подотчетность за конфиденциальность данных
- ❑ Прочее (просьба указать):

[4] Оценка воздействия на защиту данных – это процесс выявления и снижения рисков, связанных с обработкой персональных данных.

Часть III – Информационные обязательства

8. Как вы информируете субъектов персональных данных[5] о средствах и целях, для которых обрабатываются их персональные данные[6]? Пожалуйста, выберите все применимые варианты (возможно более одного ответа):

- ❑ Уведомление о конфиденциальности
- ❑ Положения и условия
- ❑ Электронная почта
- ❑ Формы согласия
- ❑ Нет
- ❑ Прочее (просьба указать):

9. Как вы гарантируете, что персональные данные обрабатываются исключительно в целях, для которых они были собраны? Пожалуйста, выберите все применимые варианты (возможно более одного ответа):

- ❑ Регулярно просматриваем и обновляем политику конфиденциальности и формы согласия в соответствии с конкретными целями сбора данных
- ❑ Обеспечиваем четкую и прозрачную коммуникацию с субъектами данных относительно предполагаемого использования их персональных данных и получаем явное согласие для любых дополнительных целей
- ❑ У нас нет определенного метода обеспечения того, чтобы персональные данные обрабатывались исключительно в целях, для которых они были собраны
- ❑ Прочее (просьба указать):

Часть IV – Конфиденциальность и безопасность обмена данными

10. Как вы предотвращаете несанкционированный обмен конфиденциальной информацией[7]? Пожалуйста, выберите все применимые варианты (возможно более одного ответа):

- ❑ Мы проводим регулярные тренинги и программы повышения осведомленности о защите данных и обязательствах по соблюдению конфиденциальности
- ❑ У нас есть письменные политика и процедуры, которые определяют роли и обязанности обработчиков данных и последствия несоблюдения
- ❑ Мы используем технические и организационные меры[8] для защиты конфиденциальной информации от несанкционированного доступа, использования, модификации или раскрытия

[5] Субъект персональных данных относится к любому отдельному лицу, которое может быть идентифицировано, прямо или косвенно, с помощью идентификатора, такого как имя, идентификационный номер, данные о местоположении, или с помощью факторов, специфичных для физической, физиологической, генетической, ментальной, экономической, культурной или социальной идентичности человека. Другими словами, субъект данных – это конечный пользователь, чьи персональные данные могут быть собраны.

[6] Обработка персональных данных означает любую операцию или набор операций, выполняемых с персональными данными, таких как сбор, хранение, использование, раскрытие или удаление.

[7] Несанкционированный обмен конфиденциальной информацией означает раскрытие или использование информации, предназначенной только для определенных физических или юридических лиц.

[8] Технические меры включают такие механизмы, как шифрование, контроль доступа для защиты информации и организационные меры, включающие внедрение процедур и практик для управления рисками, связанными с обработкой данных, и их снижения.

- ❑ Мы отслеживаем и проверяем действия по обработке данных и сообщаем о любых нарушениях или инцидентах соответствующим органам власти и сторонам
- ❑ Прочее (просьба указать):

Что касается вопросов с 11 по 15, ВПС признает, что вы можете использовать технологии и услуги, предоставляемые его Центром почтовых технологий (ЦПТ), и, в частности, Международную почтовую систему (IPS) и/или Систему таможенного декларирования (CDS), в некоторых случаях размещение программного обеспечения, также предоставляемого РТС (Облачные сервисы и .post services). В таких случаях часть ответов на приведенные ниже вопросы может быть получена из операций ЦПТ. Однако мы убедительно просим вас ответить на эти вопросы и дополнить свои ответы мерами, которые вы принимаете на местном уровне.

11. Есть ли у вас план действий в чрезвычайных ситуациях[9] и система резервного копирования для обеспечения непрерывности обслуживания и возобновления деятельности в случае незапланированного прерывания или других чрезвычайных ситуаций? (Пожалуйста, выберите только один ответ из следующих):
    - ❑ Да, у нас есть как план действий в чрезвычайных ситуациях, так и система резервного копирования
    - ❑ Нет, у нас нет плана действий в чрезвычайных ситуациях или системы резервного копирования
    - ❑ Прочее (просьба указать):

12 Как вы отслеживаете любые нарушения безопасности[10], связанные с обменом персональными данными с другими сторонами, и сообщаете о них? (Пожалуйста, выберите только один ответ из следующих):
    - ❑ У нас есть специальная группа по безопасности или подразделение, которое отслеживает любые нарушения безопасности и сообщает о них
    - ❑ У нас есть политика или процедура реагирования на нарушения безопасности, которые определяют нашу деятельность по мониторингу и отчетности
    - ❑ Мы полагаемся на функции безопасности или оповещения наших систем или сетей для обнаружения любых нарушений безопасности и сообщения о них
    - ❑ Мы не отслеживаем и не сообщаем о каких-либо нарушениях безопасности
    - ❑ Прочее (просьба указать):

13. Какие стороны вы уведомляете в случае нарушения безопасности? Пожалуйста, выберите все применимые варианты (возможно более одного ответа):
    - ❑ Международное бюро ВПС
    - ❑ Местные органы по защите данных
    - ❑ Затронутые субъекты данных
    - ❑ Затронутые контрагенты

[9] План действий в чрезвычайных ситуациях – это набор процедур и действий, направленных на предотвращение, подготовку, реагирование и восстановление после любых потенциальных угроз или сбоев, которые могут повлиять на почтовую службу, таких как стихийные бедствия, несчастные случаи или кибератаки.

[10] Нарушение безопасности – это событие, которое ставит под угрозу конфиденциальность, целостность или доступность данных, которыми обмениваются с другими сторонами, такое как несанкционированный доступ, раскрытие, модификация, потеря или уничтожение.

- ❑ Мы не уведомляем о нарушениях безопасности какие - либо другие стороны
- ❑ Прочее (просьба указать):

14. Как быстро вы уведомляете соответствующие стороны о нарушении безопасности? (Пожалуйста, выберите только один ответ из следующих):

- ❑ В течение 24 часов
- ❑ В течение 72 часов
- ❑ В течение одной недели
- ❑ В течение одного месяца
- ❑ Мы не уведомлять о любом нарушении безопасности
- ❑ Прочее (просьба указать):

15. Как часто вы проводите проверки безопасности или оценки[11] инфраструктуры и операционной среды, используемых для обмена данными с другими сторонами? (Пожалуйста, выберите только один ответ из следующих):

- ❑ Ежемесячно
- ❑ Ежеквартально
- ❑ Раз в полгода
- ❑ Ежегодно
- ❑ Никогда
- ❑ Прочее (просьба указать):

Часть V – Хранение данных

16. Как вы определяете срок хранения [12] обрабатываемых вами персональных данных? (Пожалуйста, выберите только один ответ из следующих):

- ❑ Мы соблюдаем срок хранения в соответствии с местной юрисдикцией
- ❑ Мы соблюдаем срок хранения в соответствующей юрисдикции с наиболее строгими ограничениями
- ❑ Мы храним персональные данные столько, сколько необходимо

[11] Проверка безопасности или оценки – это систематические оценки политик, процедур и средств контроля, которые защищают конфиденциальность, целостность и доступность данных, которыми обмениваются с другими сторонами.

[12] Срок хранения – это период времени, в течение которого персональные данные хранятся в целях их обработки, хранения или архивирования, прежде чем их безопасно удалить или уничтожать.

- ❑ Мы храним персональные данные в течение установленного периода в 10 лет с даты получения
- ❑ Прочее (просьба указать):

17. Как вы распоряжаетесь персональными данными[13] по истечении срока хранения или когда персональные данные больше не нужны для определенных целей? Пожалуйста, выберите все применимые варианты (возможно более одного ответа):

- ❑ Мы удаляем персональные данные со всех систем и устройств
- ❑ Мы уничтожаем персональные данные путем измельчения, сжигания или размагничивания
- ❑ Мы возвращаем персональные данные отправляющей стороне или передаем их третьей стороне, уполномоченной отправляющей стороной
- ❑ Мы анонимизируем или агрегируем персональные данные для удаления любой личной или конфиденциальной информации
- ❑ Мы храним персональные данные для архивных, исследовательских или статистических целей при соблюдении соответствующих мер предосторожности
- ❑ Прочее (просьба указать):

Часть VI – Права доступа

18. Какие права доступа субъекта данных[14] вы предоставляете? Пожалуйста, выберите все применимые варианты (возможно более одного ответа):

- ❑ Права доступа
- ❑ Право на исправление
- ❑ Право на уничтожение
- ❑ Право на переносимость данных
- ❑ Права на возражение против
- ❑ Право на ограничение обработки
- ❑ Никаких особых прав, предоставляемых
- ❑ Прочее (просьба указать):

[13] Распоряжение персональных данных означает удаление, уничтожение или обезличивание персональных данных безопасным и необратимым образом, чтобы к ним не могли получить доступ, использовать или раскрыть неуполномоченные лица.

[14] Права доступа субъекта данных – это права, которыми могут обладать физические лица на доступ, исправление, удаление или ограничение обработки своих персональных данных, хранящихся в организации

19. Насколько быстро вы отвечаете [15] на запросы от других сторон или непосредственно от субъектов данных? (Пожалуйста, выберите только один ответ из следующих):

- ❑ Течение одного календарного дня
- ❑ В течение 1-3 календарных дней
- ❑ В течение 4-7 дней
- ❑ В течение 2-3 недель
- ❑ В течение одного месяца
- ❑ Нет конкретных сроков
- ❑ Прочее (просьба указать):

20. Каким образом [16] вы отвечаете на информационные запросы от других сторон или непосредственно от субъектов данных? Пожалуйста, выберите все применимые варианты (возможно более одного ответа):

- ❑ У нас есть официальная политика и процедура оценки информационных запросов от других сторон и реагирования на них, и мы документируем и отслеживаем все запросы и ответы
- ❑ У нас есть общие рекомендации по реагированию на информационные запросы от других сторон, но у нас нет официальной политики или процедуры, и мы не документируем и не отслеживаем все запросы и ответы
- ❑ У нас нет какого-либо специального процесса для ответа на информационные запросы от других сторон, и мы обрабатываем их в индивидуальном порядке, в зависимости от характера и источника запроса
- ❑ Мы не отвечаем ни на какие информационные запросы от других сторон, за исключением случаев, когда это требуется по закону
- ❑ Прочее (просьба указать):

Часть VII – Запись действий по обработке данных

21. Как вы ведете свои записи о действиях по обработке данных[17]? Каков общий формат и структура ваших записей о действиях по обработке данных? (Пожалуйста, выберите только один ответ из следующих):

- ❑ Мы используем специальное программное обеспечение
- ❑ Мы используем электронную таблицу или документ
- ❑ Мы используем физический или электронный журнал регистрации
- ❑ Мы не ведем учет операций по обработке
- ❑ Прочее (просьба указать):

[15] Ответ – это любое сообщение, подтверждающее запрос другой стороны, дающее ответ на него или принимающее последующие меры в связи с ним, например электронное сообщение или письмо в письменной форме.
[16] Процессы реагирования на информационные запросы от других сторон могут включать такие этапы, как получение, проверка, определение приоритетов, назначение, извлечение, компиляция, обзор, утверждение и отправка информации.
[17] Записи о действиях по обработке – это документы или записи, описывающие персональные данные, которые вы собираете, используете, храните и передаете как почтовый оператор.

22. Какую информацию о действиях по обработке вы собираете в своих записях? Пожалуйста, выберите все применимые варианты (возможно более одного ответа):

- ❑ Наименование и контактные данные каждой стороны, осуществляющей обработку данных
- ❑ Категории и источники обрабатываемых данных
- ❑ Описание технических и организационных мер безопасности
- ❑ Прочее (просьба указать):

23. Как часто вы просматриваете и обновляете свои записи о действиях по обработке? (Однократный выбор):

- ❑ Не реже одного раза в год
- ❑ Каждые шесть месяцев
- ❑ Каждые три месяца
- ❑ Чаще, чем раз в три месяца
- ❑ Никогда или редко
- ❑ Прочее (просьба указать):

Часть VIII – Обучение и осведомленность

24. Проводит ли ваша организация обучение сотрудников по защите данных[18]? (Пожалуйста, выберите только один ответ из следующих):

- ❑ Да, мы проводим регулярные и комплексные учебные программы по защите данных для всех сотрудников
- ❑ Да, но обучение минимально или обновляется нерегулярно
- ❑ Нет, в настоящее время наша организация не проводит никаких тренингов по защите данных для персонала
- ❑ Прочее (просьба указать):

Часть IX – Практический опыт

25. Сталкивались ли вы когда-либо с какими-либо трудностями или вызовами[19] при сборе, обработке, передаче или получении данных? (Пожалуйста, выберите только один ответ из следующих):

- ❑ Да, часто
- ❑ Да, иногда

[18] Обучение включает в себя любой формализованный метод обучения сотрудников применимым принципам, процессам и обязанностям по теме защиты данных/конфиденциальности, включая живые тренинги, электронное обучение, ресурсы и материалы и т.д.

[19] Трудности или вызов могут включать технические проблемы, проблемы с качеством данных, нарушения безопасности данных или конфиденциальности, нормативные или правовые барьеры.

- ❑ Нет, никогда
- ❑ Я не знаю
- ❑ Прочее (просьба указать):

26. Если вы ответили утвердительно на предыдущий вопрос, каковы были основные причины или источники трудностей или вызовов? Пожалуйста, выберите все применимые варианты (возможно более одного ответа):

- ❑ Несовместимые или устаревшие технические стандарты или системы
- ❑ Отсутствие ясности или последовательности в требованиях к данным или форматах
- ❑ Юридические или нормативные барьеры или ограничения
- ❑ Человеческие или операционные ошибки или задержки
- ❑ Прочее (просьба указать):