Аналитический материал RPPA [РФ] об определении личности субъекта персональных данных при обращении к оператору

[Авторы: К.Зюбанов, Д.Прохоренко, Г.Сабиров] [Рецензенты: Н.Дмитрик, А.Мунтян, А.Партин] [Оригинал публикации]

RPPA 2025.04.21

1. Проблематика

- **Закон дает субъекту права**, но предусматривает общие требования в отношении **обращения за их реализацией** или не предусматривает их.
- **При обращении субъекта** оператор устанавливает тождественность отправителя и лица, чьи данные фактически обрабатываются.
- **Если данных в обращении недостаточно**, оператор балансирует между правами субъекта и конфиденциальностью ПД.

2. Аналитика

- **Отправитель** должен указать информацию, достаточную для его определения как субъекта, чьи ПД предположительно обрабатываются.
- **Определение отправителя** как процесс – **обработка ПД**, к ней применяется принцип минимизации, не допускающий избыточную обработку ПД.
- **Использование функционала онлайн-сервиса (например, личного кабинета)** для реализации прав решает задачу подтверждения тождественности; в иных случаях при отсутствии в обращении необходимых идентификаторов субъекта требуется принятие доп мер.
  - **Например,** даже предоставление реквизитов паспорта может оказаться недостаточным и нецелесообразным в случаях, когда речь идет об обработке адреса электронной почты для рекламных рассылок или данных файлов cookie для аналитики.

- **Данный материал наиболее актуален для онлайн-сервисов, но** подходит и для иных случаев обработки ПД.
- **Материал кросс-юрисдикционен**, но рекомендуется обратиться к применимому законодательству, судебной практике и разъяснениям регуляторов.
- **Подтверждения тождественности** – это определение соответствия отправителя обращения конкретному субъекту ПД.

3. Эврика

- **Чтобы верно установить набор сведений,** необходимых для решения задачи подтверждения тождественности, следует учитывать **контекст обработки ПД.**
- **Если установленные законом требования к обращению не исполнены**, ни отказ в удовлетворении, ни исполнение требования субъекта сами по себе не будут нарушением.
- **При решении задачи подтверждения тождественности** нужно исходить из целесообразности принятия дополнительных мер и уровня риска для прав субъекта при удовлетворении требования отправителя.
- **При оценке указанной целесообразности и уровня риска** необходимо учитывать, в частности, объем данных в обращении, возможное влияние исполнения требования на обработку и (или) права субъекта.

Доп. меры / Риск субъекта	Целесообразны	Нецелесообразны
Высокий	Принять доп. меры	Мотивированно отказать в удовлетворении
Низкий	Удовлетворить требование / принять доп. меры	Удовлетворить требования отправителя

- **Лучшие практики для операторов и примеры дополнительных мер**:

✓ предоставление отправителю мотивированного ответа на обращение в любом случае;
✓ публикация правил обращения (например, в политике конфиденциальности) с учётом возможных проблем определения отправителя как конкретного субъекта ПД;
✓ построение процесса работы с обращениями для обеспечения надлежащих и оперативных ответов отправителям;
✓ обеспечение возможности реализации прав субъектов в самом онлайн-сервисе (например, возможность доступа к редактированию/удалению ПД через личный кабинет сервиса без обращения к оператору);
✓ использование OTP (one-time password – *одноразовый пароль*) для подтверждения связи отправителя с конкретной учетной записью при обращении вне онлайн-сервиса;
✓ использование 2FA, MFA и иных подобных способов для подтверждения связи отправителя с субъектом (например, через запрос второго фактора);
✓ использование сторонних сервисов аутентификации как «гарантов» тождественности;
✓ обеспечение возможности отзыва согласия в каждой маркетинговой коммуникации;
✓ запрос дополнительной информации, отсутствующей в обращении, но имеющейся в распоряжении оператора (например, данные личного кабинета сервиса или «кодовая фраза»).