Kept GDPR Day

25 мая 2023 г.

kept

GDPR сегодня: трендсеттер в мире приватности?

Ксения Карпова
менеджер, Группа по оказанию услуг в области кибербезопасности и цифровой криминалистики, Kept

Тренды, заданные GDPR

kept

Что нового принёс GDPR?

Экстерриториальность

GDPR применим **даже к компаниям за пределами ЕЭЗ** при условии, что компания:

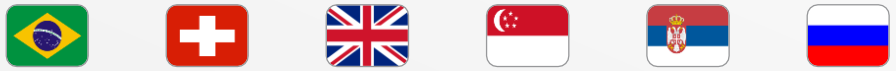
- предлагает товары и услуги субъектам ПДн, находящимся в ЕЭЗ, независимо от их стоимости, либо
- осуществляет мониторинг поведения субъектов ПДн, если такое поведение происходит в ЕЭЗ

Оборотные штрафы

GDPR ввел штрафы в размере 20 млн евро или **оборотный штраф** до 4% от годового дохода компании, в зависимости от того, какая сумма выше

Ужесточение требований к трансграничной передаче

- GDPR предусматривает список стран, обеспечивающих адекватный уровень защиты ПДн
- При передаче в страны с неадекватным уровнем защиты ПДн, необходимо обеспечить д**ополнительные гарантии безопасности ПДн** и провести **оценку воздействия трансграничной передачи ПДн на субъекта (TIA)**



Data Protection Officer (DPO)

GDPR ввел термин Data Protection Officer (DPO) – должностное лицо, отвечающее за соблюдение компанией требований GDPR. При этом к DPO применяются в том числе требования по отсутствию конфликта интересов должностей, прямому доступу к руководству и отсутствию административной ответственности

Исследование IAPP

Исследование Kept мирового законодательства по приватности

90 Юрисдикций

Более 90 юрисдикций были изучены нашей командой на наличие законодательства по приватности

16 Законов с экстерриториальностью

В 16 странах / регионах были выявлены критерии экстерриториальности

27 Законов с локализацией

В 24 странах / регионах были выявлены требования по локализации баз данных на территории страны, при этом в Турции было выявлено 4 закона, содержащие такие требования

Страны / регионы с экстерриториальной применимостью з-ва: ЕЭЗ, Великобритания, Япония, Турция, Таиланд, Швейцария, Нигерия, Египет, Китай, США (Калифорния, Колорадо, Юта, Невада), Бразилия, Российская Федерация, ОАЭ

Критерии

Блок 1:

Обработка субъектов в другой стране связана с:

(a) предложением товаров и / или услуг вне зависимости от того, требуется ли оплата

(b) мониторингом поведения

Блок 2:

(a) обработка ПДн граждан другой страны, или

(b) обработка субъектов, находящихся на территории другой страны

Страны / регионы с требованиями по локализации : Австралия, Алжир, Кения, Казахстан, Пакистан, Нигерия, Турция, Руанда, Узбекистан, Южная Корея, Шри-Ланка, Российская Федерация, Вьетнам, Дания, Индия, Канада, Китай, Люксембург, Саудовская Аравия, Болгария, Польша, Румыния, Япония, Швейцария

Ограничения сферы деятельности компании при локализации: Медицинские учреждения, Платформы электронной коммерции, Стратегические интересы государства (КИИ), Банки и финансовые учреждения, Государственные органы, Поставщики телекоммуникационных и интернет услуг, Игорный бизнес, Владельцы социальных сетей

И это все тренды?

- **Легитимный интерес**
- **Разъяснения регуляторов**
- **Усиление требований к согласию**
- **Запрет cookie wall**
- **privacy by design and by default**
- **Право на забвение и право на перенос данных**
- **Обязательное уведомление регулятора и пострадавших субъектов при нарушении безопасности ПДн**
- **И многое другое…**

Обзор самых громких и интересных штрафов за последний год

Иван Агафонов
консультант, Группа по оказанию услуг в области кибербезопасности и цифровой криминалистики, Kept

Анна Чеботарева
консультант, Группа по оказанию услуг в области кибербезопасности и цифровой криминалистики, Kept

Статистика по штрафам за последний год

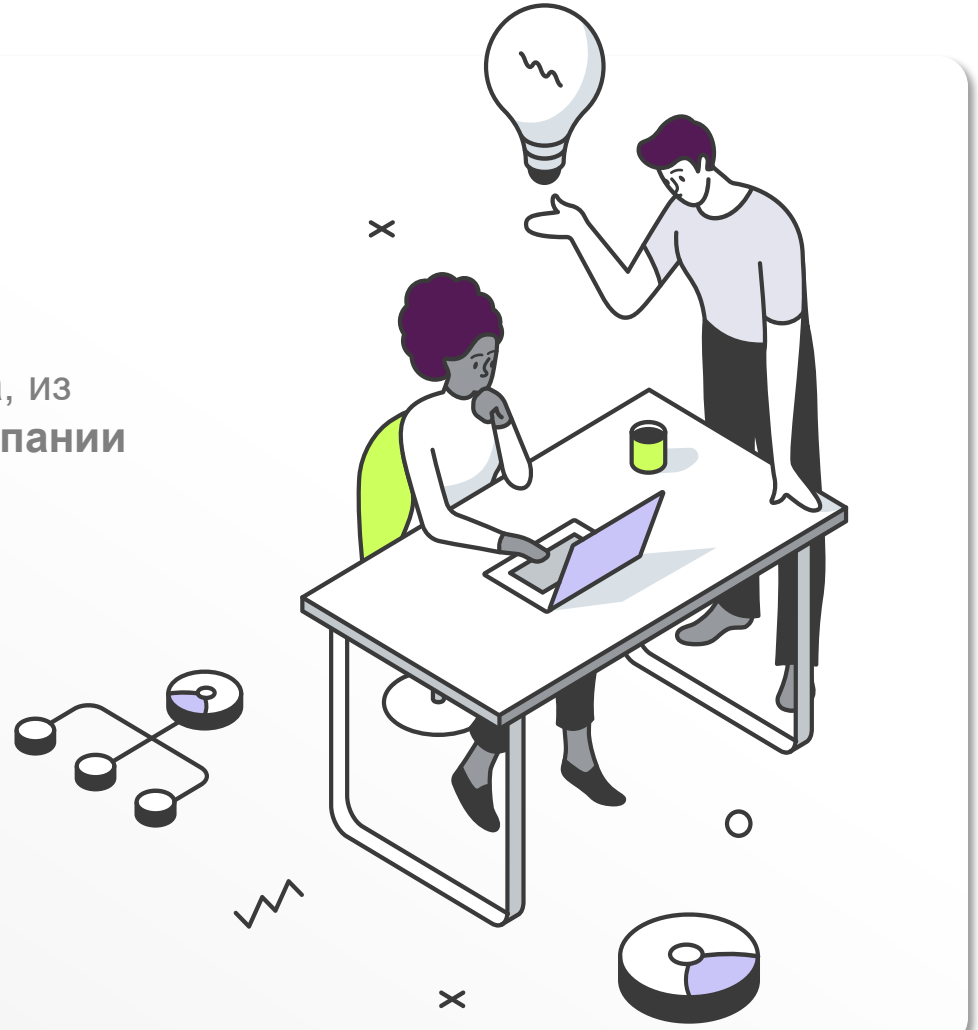
Статистика по штрафам за последний год (май 2022 – май 2023 года)

Более
530
штрафов

Более
500
штрафов
на сумму **меньше 500 тыс евро**

Более
30
штрафов
на сумму от **500 тыс евро**

Более
70
штрафов
выписано на **физические лица**, из них более **60 в Испании**



Статистика по штрафам за последний год (май 2022 – май 2023 года)

Топ самых крупных штрафов

№	Компания	Регулятор и ссылка на штраф	Сумма штрафа, евро
1	Meta* Platforms Ireland Limited	Ирландия (DPC)	1,2 млрд
2		Ирландия (DPC)	390 млн
3		Ирландия (DPC)	265 млн
4	Meta* Platforms, Inc	Ирландия (DPC)	405 млн
5	Clearview AI Inc	Франция (CNIL), Греция (HDPA), Италия (GPDP)	от каждого регулятора по 20 млн
6	Google LLC	Испания (AEPD)	10 млн
7	WhatsApp Ireland Ltd	Ирландия (DPC)	5,5 млн
8	Edison Energia S.p.A.	Италия (GPDP)	4,9 млн
9	Portuguese National Statistical Institute	Португалия (CNPD)	4,3 млн
10	Debt collection agency	Хорватия (AZOP)	2,3 млн

Топ стран с самым большим количеством штрафов

Испания (AEPD)
более **240** штрафов

Италия (GPDP)
более **100** штрафов

Румыния (ANSPDCP)
более **60** штрафов

** Организация, деятельность которой запрещена на территории Российской Федерации*

Самые громкие штрафы за последний год*

*период май 2022 – май 2023 года

Штрафы, наложенные на Meta*

kept

Самая штрафуемая компания

Общая сумма штрафов, наложенных на Meta в 2022 году, превышает **687 млн. €**

Крупнейший штраф в истории

22 мая 2023 г. на Meta был наложен крупный штраф в размере **1,2 млрд. €.** Штраф был наложен за передачу ПДн европейцев в США без надлежащих мер для их защиты от незаконного доступа американских спецслужб

Описание штрафов

Штрафы накладывались за повторные нарушения, а также за нарушения, которые были выявлены в дочерних компаниях Meta

Как избежать

Оперативно исправлять выявленные регулятором нарушения и реагировать на его запросы. Внедрить инструменты контроля соответствия требованиям применимого законодательства по приватности

** Организация, деятельность которой запрещена на территории Российской Федерации*

Наиболее частое нарушение

Discord Inc. (крупный мессенджер)

Надзорный орган

CNIL (Франция)

Размер штрафа

800 000 €

Нарушенные статьи GDPR

5 (1) e), 13, 25 (2), 32, 35

Источник

–

Описание

- Компания не установила, а также не соблюдала срок хранения ПДн, соответствующий цели обработки
- В базе данных насчитывалось более 2 000 000 учетных записей французских пользователей, которые не пользовались своей учетной записью более трех лет, и примерно 50 000 учетных записей, которые не использовались более пяти лет

Как избежать

- Установить сроки хранения ПДн
- Внедрить механизмы уничтожения ПДн по истечению срока хранения

Штрафуют даже искусственный интеллект

Clearview AI Inc. (компания, разрабатывающая ИИ)

Надзорный орган

CNIL (Франция)
HDPA (Греция)
IDPA (Италия)

Размер штрафа

20 000 000 €

Нарушенные статьи GDPR

5 (1) a), b), e), 6, 9, 12, 13, 14, 15, 27

Источник

–

Описание

- В ходе своего расследования регуляторы установили, что ПДн, содержащиеся в базе данных компании (более 20 млрд. фотографий, полученных из соц. сетей), были обработаны без правовых оснований
- Кроме того, регуляторы обнаружили, что компания ограничивала осуществление прав субъектов ПДн

Как избежать

- Обеспечить получение правовых оснований для всех целей обработки ПДн

Нарушение основных принципов GDPR (Испания)

Различные организации и физические лица

Надзорный орган

AEPD (Испания)

Размер штрафа

180 – 525 000 €

Нарушенные статьи GDPR

5 (1) c, 5 (1) f

Кол-во штрафов:

более 120*

Источник

Жалоба субъекта ПДн

Описание

- Контролер запросил излишний объем ПДн (номера ID карт) с целью регистрации на мероприятие
- Контролер (физическое лицо) установил камеры видеонаблюдения, которые охватывали общественное пространство и соседнюю собственность
- Контролер отправил электронное письмо с ПДн нескольким получателям из открытого списка рассылки

Как избежать

Проводить периодический анализ соответствия целей обработки ПДн и обрабатываемых ПДн, прекращать обработку избыточных категорий ПДн при отсутствии цели на их обработку

* Было выписано более 120 штрафов из них более 50 на физические лица, другие на организации

Нарушение основных принципов GDPR (Италия)

Различные организации и физические лица

Надзорный орган

GPDP (Италия)

Размер штрафа

1 000 – 4 900 000 €

Нарушенные статьи GDPR

5 (1), 6, 7, 9

Кол-во штрафов:

более 80

Источник

–

Описание

- Рекламные сообщения были отправлены субъектам ПДн без их согласия
- Контролер использовал камеры видеонаблюдения в своих помещениях, о чем не уведомил субъектов ПДн
- Маркетинговая компания не смогла продемонстрировать наличие правового основания для обработки данных 21 млн человек, собранных через различные онлайн-порталы для маркетинговой деятельности
- Муниципалитет опубликовал на своем веб-сайте документ, содержащий ПДн сотрудника, без правового основания
- Контролер установил систему видеонаблюдения, которая охватывала дорогу общего пользования и частную собственность, о чём субъекты ПДн не были проинформированы

Нарушение основных принципов GDPR, неисполнение прав субъектов ПДн (Италия)

Edison Energia S.p.A.

Надзорный орган

GPDP (Италия)

Размер штрафа

4 900 000 €

Нарушенные статьи GDPR

5 (1, 2), 6, 7, 9, 12

Кол-во штрафов:

1

Источник

Жалоба субъекта ПДн

Описание

- Субъекты ПДн подали жалобы на незаконную маркетинговую деятельность компании
- Компания не предоставила субъектам ПДн прямого и простого способа реализовать свое право на возражение против обработки ПДн
- Компания своевременно не ответила на запросы субъектов ПДн
- Пользователи приложения и веб-сайта одновременно дали согласие на использование ПДн как в маркетинговых целях, так и в целях профилирования
- Компания не предоставила субъектам ПДн прозрачную информацию об обработке их ПДн

Как избежать

- Обеспечить наличие правовых оснований для всех целей обработки ПДн
- Разработать механизмы реализации прав субъектов ПДн
- Разработать механизм ответа на запросы субъектов ПДн

Неисполнение прав субъектов ПДн

Различные организации

Надзорный орган

AEPD (Испания)

Размер штрафа

600 – 40 000 €

Нарушенные статьи GDPR

15, 17, 28

Кол-во штрафов:

менее 10

Источник

Жалоба субъекта ПДн

Описание

- Контролеры должным образом не выполнили запросы субъектов ПДн о доступе и удалении их персональных данных.
- Субъект ПДн получил рекламный звонок от контролера, сделанный от имени Vodafone España, S.A.U., хотя субъект ПДн был зарегистрирован в списке исключений для рекламы

Как избежать

Разработать механизм ответа на запросы субъектов ПДн и контролировать его исполнение

Неисполнение прав субъектов ПДн ●●

kept

Различные организации

Надзорный орган

GPDP (Италия)

Размер штрафа

1 – 70 тыс €

Нарушенные статьи GDPR

12, 15

Кол-во штрафов:

более 15

Источник

Жалоба субъекта ПДн

Описание

- Субъект ПДн подал жалобу GPDP, утверждая, что его право на доступ к своим ПДн не было соблюдено в достаточной степени
- Компания потребовала заполнить специальную форму, чтобы получить доступ к ПДн, что непропорционально затрудняло осуществление права доступа
- Сотрудник контролера запросил доступ к своим ПДн, обрабатываемых в контексте их трудовых отношений. Но контролер не смог своевременно выполнить этот запрос
- Контролер несвоевременно предоставил ответ на запрос субъекта ПДн о доступе к его данным

Как избежать

Разработать механизм ответа на запросы субъектов ПДн и контролировать его исполнение

Отсутствие законных оснований обработки ПДн

Vodafone España, S.A.U.

Надзорный орган

AEPD (Испания)

Размер штрафа

40 – 136 тыс €

Нарушенные статьи GDPR

6 (1), 32

Кол-во штрафов:

более 10

Источник

Жалоба субъекта ПДн

Описание

- Компания предоставила дубликат SIM-карты субъекта ПДн другому лицу, которое получило доступ к банковскому счету субъекта
- Контролер провел проверку кредитоспособности физического лица, не имея с ним никаких договорных отношений
- Неавторизованные мошенники получили доступ к учетной записи Vodafone и внесли изменения в договор

Как избежать

Внедрить технические меры, позволяющие проводить авторизацию субъекта ПДн при получении запроса от субъекта ПДн и определять релевантность запроса

Отсутствие сотрудничества с регулятором

Различные организации

Надзорный орган

AEPD (Испания)

Размер штрафа

600 – 25 000 €

Нарушенные статьи GDPR

58 (1, 2)

Кол-во штрафов:

менее 10

Источник

–

Описание

- Компания не выполнила приказ, изданный AEPD
- Компания не предоставила информацию по запросу AEPD в ходе проводимого расследования
- Контролер не внедрил в установленный срок меры, неоднократно предписываемые AEPD

Как избежать

Оперативно реагировать на выявленные регулятором нарушения и отвечать на его запросы

Недостаточные меры защиты ПДн (Италия)

kept

Различные организации

Надзорный орган

GPDP (Италия)

Размер штрафа

3 – 120 тыс €

Нарушенные статьи GDPR

32

Кол-во штрафов:

менее 20*

Источник

Жалоба субъекта ПДн

Описание

- Компания по ошибке отправила документ, содержащий данные о состоянии здоровья субъекта ПДн, другому субъекту
- Субъект ПДн подал жалобу регулятору, получив медицинскую карту другого субъекта ПДн
- Сотрудники медицинского учреждения получили доступ к медицинским данным пациентов, хотя они не участвовали в лечении этих пациентов и такой доступ им не требовался

Как избежать

Предпринять надлежащие технических и организационных меры для обеспечения уровня безопасности защиты ПДн, соответствующего риску

* из них более 10 на организации в сфере здравоохранения

Штраф на государственную организацию

Italian Ministry of Defense (Министерство обороны Италии)

Надзорный орган

GPDP (Италия)

Размер штрафа

10 тыс €

Нарушенные статьи GDPR

5 (1) a, 6, 9, 10

Источник

Жалоба субъекта ПДн

Описание

- GPDP получил жалобу от субъекта ПДн (сотрудник Министерства обороны Италии)
- В ходе своего расследования GPDP обнаружил, что два электронных письма были пересланы без авторизации субъекта ПДн. Эти электронные письма содержали, в том числе сведения о состоянии здоровья субъекта ПДн и сведения о судебных разбирательствах

Как избежать

- Внедрить технические меры, позволяющие проводить авторизацию субъекта ПДн при получении запроса от субъекта ПДн и определять релевантность запроса
- Разработать механизм ответа на запросы субъектов ПДн и контролировать его исполнение

Порядок наложения штрафов в соответствии с разъяснениями EDPB

kept

01

Шаг 1

Определение процесса обработки ПДн и оценка применения к нему ст. 83(3) GDPR

02

Шаг 2

Определение базового уровня штрафа для дальнейшего расчета на основе оценки:

а) общих условий, указанных в ст. 83-86 GDPR

б) серьезности нарушения

в) оборота компании

Порядок наложения штрафов в соответствии с разъяснениями EDPB

kept

03

Шаг 3

Оценка отягчающих и смягчающих обстоятельств, связанных с прошлым или настоящим поведением контролера / процессора, и соответствующее увеличение или уменьшение штрафа

04

Шаг 4

Определение максимально возможной суммы штрафа для каждого из процессов обработки ПДн

05

Шаг 5

Анализ того, соответствует ли окончательная сумма начисленного штрафа требованиям эффективности, сдержанности и соразмерности, как того требует статья 83(1) GDPR, и соответствующее увеличение или уменьшение штрафа

Проблемы трансграничной передачи персональных данных в международных компаниях

Яна Гришкова
консультант, Группа по оказанию услуг в области кибербезопасности и цифровой криминалистики, Kept

Почему важно обеспечивать соответствие требованиям при трансграничной передаче ПДн?

kept

Штрафы,

предусмотренные за нарушение требований законодательства в процессах трансграничной передачи ПДн в соответствии с требованиями GDPR

20 млн евро,

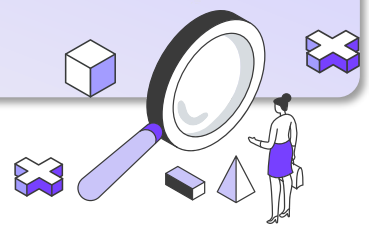
или до

4%

от годового глобального оборота за предыдущий финансовый год

Потеря доверия клиентов

Репутационные риски



Используемые термины

kept

Компания-экспортер

Компания (контроллер или процессор ПДн в зависимости от роли в процессе), обеспечивающая трансграничную передачу ПДн импортеру

Компания-импортер

Компания (контроллер или процессор ПДн в зависимости от роли в процессе), получающая ПДн от экспортера ПДн в рамках трансграничной передачи ПДн

Третья страна

Страна, находящаяся за пределами применимой юрисдикции по отношению к экспортеру ПДн

Страна, обеспечивающая адекватный уровень защиты

Страна, обеспечивающая адекватный уровень защиты данных в соответствии с решением, принятым уполномоченным надзорным органом по защите данных в применимой юрисдикции

Трансграничная передача ПДн

- **Трансграничная передача ПДн – это передача ПДн в третьи страны или международным организациям. Трансграничная передача ПДн регулируется требованиями главы V GDPR.**
- **В соответствии с Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, EDPB (European Data Protection Board) выделяет три основных критерия для определения трансграничной передачи:**

01 Компания-экспортер подпадает под действие требований GDPR в рамках рассматриваемой передачи ПДн

02 Компания-экспортер раскрывает ПДн компании-импортеру путем передачи ему ПДн субъекта

03 Компания-импортер находится в третьей стране или является международной организацией вне зависимости от того, подпадает ли она под действие GDPR

Трансграничная передача ПДн

kept

Третья страна *обеспечивает* адекватный уровень защиты ПДн

В соответствии со статьей 45 GDPR, для передачи ПДн в страны, обеспечивающие адекватный уровень защиты ПДн, **не требуется применение специальных мер, направленных на соблюдение требований, связанных с передачей ПДн в третьи страны**

Третья страна *не обеспечивает* адекватный уровень защиты ПДн

В соответствии со статьей 46 GDPR, в случае если стана не обеспечивает адекватный уровень защиты ПДн, компания-экспортер может передавать ПДн в третью страну или международную организацию, только если компания-экспортер обеспечивает соответствующие гарантии, т.е. используется корректное правовое основание для передачи ПДн:

- Standard contractual clauses (SCC);
- Binding corporate rules (BCR);
- Code of conduct (CC);
- Сертификация (Certification mechanism);
- инструмент между органами государственной власти или ведомствами, имеющий обязательную юридическую силу и обязательный к исполнению

В соответствии со статьей 49 GDPR, возможна передача в следующих случаях:

- Явное согласие субъекта ПДн;
- Выполнение договора, стороной которого является субъект ПДн;
- Общественный интерес;
- Осуществление/оспаривание судебного иска;
- Защита жизненно важных интересов субъекта;
- Передача информации из реестра, целью которого является предоставление информации общественности;
- Точечная передача ПДн ограниченного количества субъектов

Требуется проведение TIA

Кейсы из практики экспертов Kept

Кто: Группа компаний, занимающаяся сбытом продукции, производящейся на территории РФ

Задачи:

- Формирование функции приватности в целях исполнения требований GDPR и применимого локального законодательства в области приватности в компаниях Группы.
- Обеспечение возможности осуществления легитимной передачи ПДн внутри Группы компаний, а также при взаимодействии компаний Группы с российскими контрагентами

Исследуемые юрисдикции

Третьи страны

- Бразилия
- ЮАР
- Швейцария
- Сингапур
- Сербия

ЕЭЗ

- Франция
- Германия
- Кипр
- Литва
- Румыния

Кто: ИТ-интегратор, оказывающий услуги разработки ПО для более чем 70 компаний Группы, находящихся в странах по всему миру.

Задачи:

- Формирование функции приватности в целях исполнения применимого локального законодательства в области приватности в рамках разрабатываемой информационной системы.
- Обеспечение возможности осуществления легитимной передачи ПДн в рамках разрабатываемой информационной системы, а также при взаимодействии с головной компанией, расположенной в РФ

Регионы присутствия компаний Группы

- Южная Азия
- Северо-Восточная Африка
- Юго-Восточная Европа

Порядок обеспечения соответствия требованиям законодательства при трансграничной передаче ПДн

kept

01 Инвентаризация процессов, в рамках которых происходит передача ПДн

02 Определение требований применимого законодательства при передаче ПДн

03 Определение используемых инструментов передачи ПДн

04 Проведение оценки воздействия передачи ПДн на субъекта ПДн при трансграничной передаче ПДн (TIA)

05 Доведение информации об осуществлении трансграничной передачи ПДн до субъектов ПДн

Инвентаризация процессов, в рамках которых происходит передача ПДн в международных компаниях

kept

Задача:

Определить процессы, в рамках которых происходит трансграничная передача ПДн, а также роли компаний, участвующих в процессах обработки ПДн

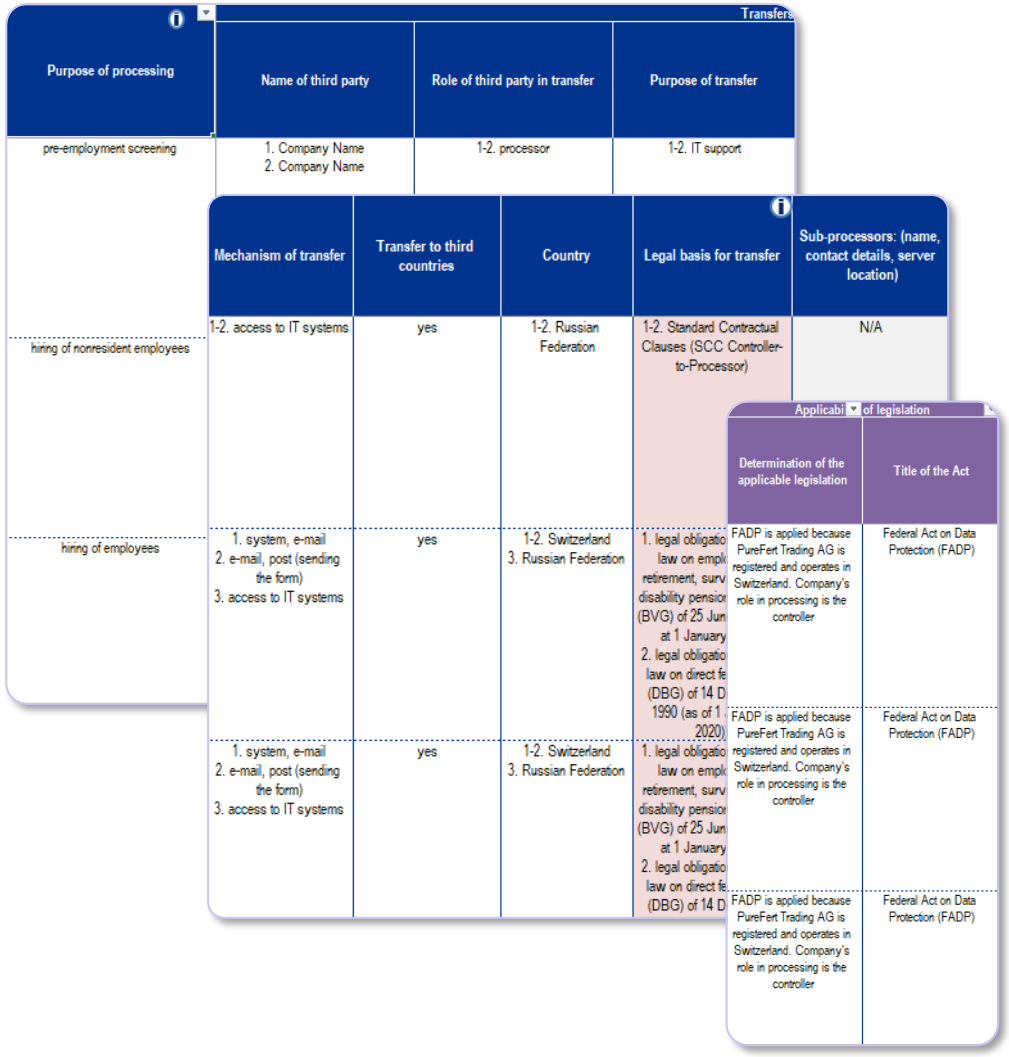
Проблема:

При взаимодействии внутри компаний Группы возможны сложности с выявлением процессов трансграничной передачи ПДн, что может быть связано с тем, что работники компаний Группы взаимодействуют между собой, не разграничивая потоки данных и не замечают факта осуществления трансграничной передачи ПДн

Решение:

Разработка реестра процессов обработки ПДн, содержащего подробную информацию об обеспечении передачи ПДн в рамках рассматриваемых процессов обработки.

При этом необходимо определить в реестре следующую информацию о передаче: наименование компаний-импортеров, их роль в процессах обработки ПДн, цель и механизм передачи, правовые основания передачи, а также меры, применяемые для обеспечения защиты ПДн субъектов в рамках процессов передачи ПДн



Purpose of processing	Transfers: Name of third party	Role of third party in transfer	Purpose of transfer	Mechanism of transfer	Transfer to third countries	Country	Legal basis for transfer	Sub-processors: (name, contact details, server location)	Applicability of legislation: Determination of the applicable legislation	Title of the Act
pre-employment screening	1. Company Name 2. Company Name	1-2. processor	1-2. IT support							
hiring of nonresident employees				1-2. access to IT systems	yes	1-2. Russian Federation	1-2. Standard Contractual Clauses (SCC Controller-to-Processor)	N/A		
hiring of employees				1. system, e-mail 2. e-mail, post (sending the form) 3. access to IT systems	yes	1-2. Switzerland 3. Russian Federation	1. legal obligatio law on empl retirement, surv disability pensio (BVG) of 25 Jun at 1 January 2. legal obligatio law on direct fe (DBG) of 14 D 1990 (as of 1 2020)	FADP is applied because PureFert Trading AG is registered and operates in Switzerland. Company's role in processing is the controller	Federal Act on Data Protection (FADP)	
				1. system, e-mail 2. e-mail, post (sending the form) 3. access to IT systems	yes	1-2. Switzerland 3. Russian Federation	1. legal obligatio law on empl retirement, surv disability pensio (BVG) of 25 Jun at 1 January 2. legal obligatio law on direct fe (DBG) of 14 D	FADP is applied because PureFert Trading AG is registered and operates in Switzerland. Company's role in processing is the controller	Federal Act on Data Protection (FADP)	
								FADP is applied because PureFert Trading AG is registered and operates in Switzerland. Company's role in processing is the controller	Federal Act on Data Protection (FADP)	

Определение требований применимого законодательства при трансграничной передаче ПДн в международных компаниях

kept

Задача:

Определить требования применимого законодательства, которые могут оказать влияние на обеспечение трансграничной передачи ПДн субъектов

Проблема:

Возможны сложности, связанные со структурированием информации при определении требований для Группы компаний, которые могут возникнуть в связи с тем, что необходимо анализировать требования не только страны-экспортера, но и страны-импортера

Решение:

Составление матрицы, содержащей положения применимого законодательства, которая является единым структурированным перечнем всех требований, которые предъявляются к компаниям Группы. В рамках матрицы есть возможность определения схожих требований, которые могут применяться сразу к нескольким юрисдикциям, а также выделения оригинальных требований

Domain	Control	Requirement	GDPR	Level of compa
Processes, procedures and technologies	Compliance with the principles of transboundary transmission of PD	The controller of the data file shall inform the Commissioner prior to transborder disclosure with regard to the safeguards and data protection rules (sufficient safeguards, in particular contractual clauses, that ensure an adequate level of protection abroad and data protection rules that ensure an adequate level of protection within the same legal person or company or between legal persons or companies that are under the same management). If information cannot be provided in advance, it must be provided immediately after disclosure	No	N/A
		If the Commissioner has been informed of the safeguards and the data protection rules, the duty to provide information for all additional disclosures is regarded as fulfilled if such disclosures: a. are made subject to the same safeguards, provided the categories of recipient, the purpose the processing and the data categories remain essentially unchanged; or b. take place within the same legal person or company or between legal persons or companies that are under the same management, provided the data protection rules continue to ensure an adequate level of protection	No	N/A
		The duty to provide information is also regarded as fulfilled if data is transmitted on the basis of model contracts or standard contract clauses that have been drawn up or approved by the Commissioner, and the Commissioner has been informed about the use of these model contracts or standard contract clauses by the controller of the data file. The Commissioner shall publish a list of the model contracts and standard contract clauses that he has drawn up or approved	No	N/A
		The controller of the data file shall take appropriate measures to ensure that the recipient complies with the safeguards and the data protection rules	No	N/A
		The Commissioner examines the safeguards and the data protection rules that have been notified to him and notifies the controller of the data file of the result of his examination within 30 days of receipt of the information	No	N/A
		The Commissioner shall publish a list of the states whose legislation ensures an adequate level of protection	No	N/A
		PD may be disclosed abroad if the Federal Council has determined that the legislation of the state concerned or the international body guarantees adequate protection	No	N/A
		If the Federal Council has not made a decision in accordance with paragraph 1, PD may be disclosed abroad if suitable data protection is guaranteed by:	No	N/A
		an international treaty	No	N/A
		Data protection clauses in a contract between the person responsible or the processor and his or her contractual partner, which the FDPIC has been notified of in advance	No	N/A
		specific guarantees drawn up by the competent federal body and communicated to the FDPIC, in	No	N/A
		Standard data protection clauses that the FDPIC has approved, issued or recognised in advance; or	No	N/A
		Binding internal company data protection regulations that have been approved in advance by the FDPIC or by an authority responsible for data protection in a country that ensures adequate protection	No	N/A
		The Federal Council may provide other suitable guarantees within the meaning of paragraph 2	No	N/A
		Notwithstanding Article 16 paragraphs 1 and 2, PD may be disclosed abroad in the following cases:	No	N/A
		The person concerned has expressly consented to the disclosure	No	N/A
		The disclosure is directly related to the conclusion or execution of a contract: 1. between the controller and the data subject; or 2. between the person responsible and his contractual partner in the interest of the data subject	No	N/A
		The notification is necessary for: 1. safeguarding an overriding public interest; or 2. establishing, exercising or enforcing legal claims before a court or other competent foreign authority	No	N/A
		Disclosure is necessary to protect the life or physical integrity of the data subject or of a third party and it is not possible to obtain the data subject's consent within a reasonable time	No	N/A
		The data subject has made the data generally accessible and has not expressly prohibited processing	No	N/A
		The data comes from a register provided for by law, which is accessible to the public or to persons with a legitimate interest, provided that the legal requirements for inspection are met in the individual case	No	N/A
		Upon request, the person responsible or the processor shall inform the FDPIC about the disclosure of PD in accordance with paragraph 1 letters b number 2, c and d.	No	N/A
		If PD is made generally accessible for public information by means of automated information and		

Определение используемых инструментов передачи ПДн при передаче ПДн между компаниями Группы

kept

Задача:

Определить инструменты передачи ПДн, использование которых будет обеспечивать соответствие требованиям применимого законодательства

Проблема:

Возможны сложности, связанные с отсутствием утвержденными надзорными органами шаблонов, используемых в качестве инструментов передачи ПДн между компаниями Группы

Решение:

В случае отсутствия инструментов, утверждённых надзорным органом применимой юрисдикции, возможно использование адаптированных версий шаблонов, утверждённых Европейской комиссией, как “best practice” в области приватности.

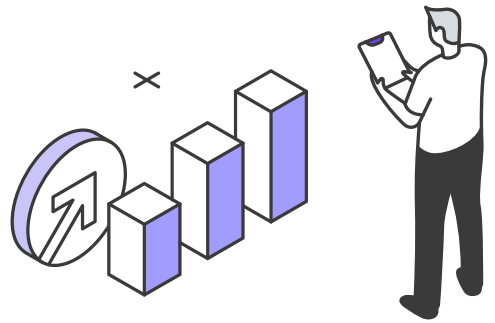
При этом под «адаптаций» понимается дополнение требованиями применимого законодательства, которые могут повлиять на процессы передачи ПДн.

Вид SCC/DTA	Область применения
SCC for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679	Передача ПДн между компаниями в ЕС/ЕЭЗ и компаниями за пределами ЕС/ЕЭЗ от
Serbian SCC for data transfers between controllers and processors	Передача ПДн от контроллера процессору в Сербии
Serbian SCC adapted to the requirements of SCC for the transfer of personal data to third countries pursuant to Regulation (EU)	Передача ПДн между компанией-контроллером в ЕС/ЕЭЗ и компанией-процессором в Сербии
SCC for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 adapted to the requirements of FADP	Передача ПДн между компанией-контроллером в Швейцарии и компанией-процессором в третьей стране
SCC between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725 adapted to the requirements of FADP	Передача ПДн от контроллера процессору в Швейцарии
Data Transfer Agreement (DTA)	Передача ПДн между двумя компаниями-контроллерами: 1. в другую юрисдикцию, в отношении которой принято решение об адекватности на основании применимого законодательства, 2. в организацию, находящуюся в той же юрисдикции, что и экспортер данных

Проведение оценки воздействия передачи ПДн на субъекта ПДн при трансграничной передаче (TIA)

Задача:

Провести оценку обеспечение безопасности ПДн при их трансграничной передаче



Порядок проведения:

Определить перечень процессов, в рамках которых происходит передача ПДн в страны, не обеспечивающие адекватный уровень защиты прав и свобод субъектов ПДн

Определить, есть ли в законодательстве страны-импортера **факторы, которые могут повлиять на обеспечение безопасности при передаче ПДн**

Внедрить «**дополнительные меры**» защиты, использующиеся при передаче в неадекватные страны

Определить правовое основание для трансграничной передачи с учетом требований, предъявляемых применимым законодательством страны-импортера и страны-экспортера

Определить «**дополнительные меры**» защиты ПДн при передаче в неадекватные страны с учетом:

- **формата передаваемых ПДн**;
- **категорий передаваемых ПДн;**
- **продолжительность и сложность процесса обработки ПДн и др.**

Осуществлять **мониторинг соблюдения требований на регулярной основе**, в том числе отслеживать и учитывать изменения, связанные с изменениями законодательства и другими соответствующими событиями, которые могут оказать влияние на передачу ПДн

Доведение информации об осуществлении трансграничной передачи ПДн до субъектов ПДн

kept

Задача:

Довести до субъекта ПДн информацию о трансграничной передаче его ПДн

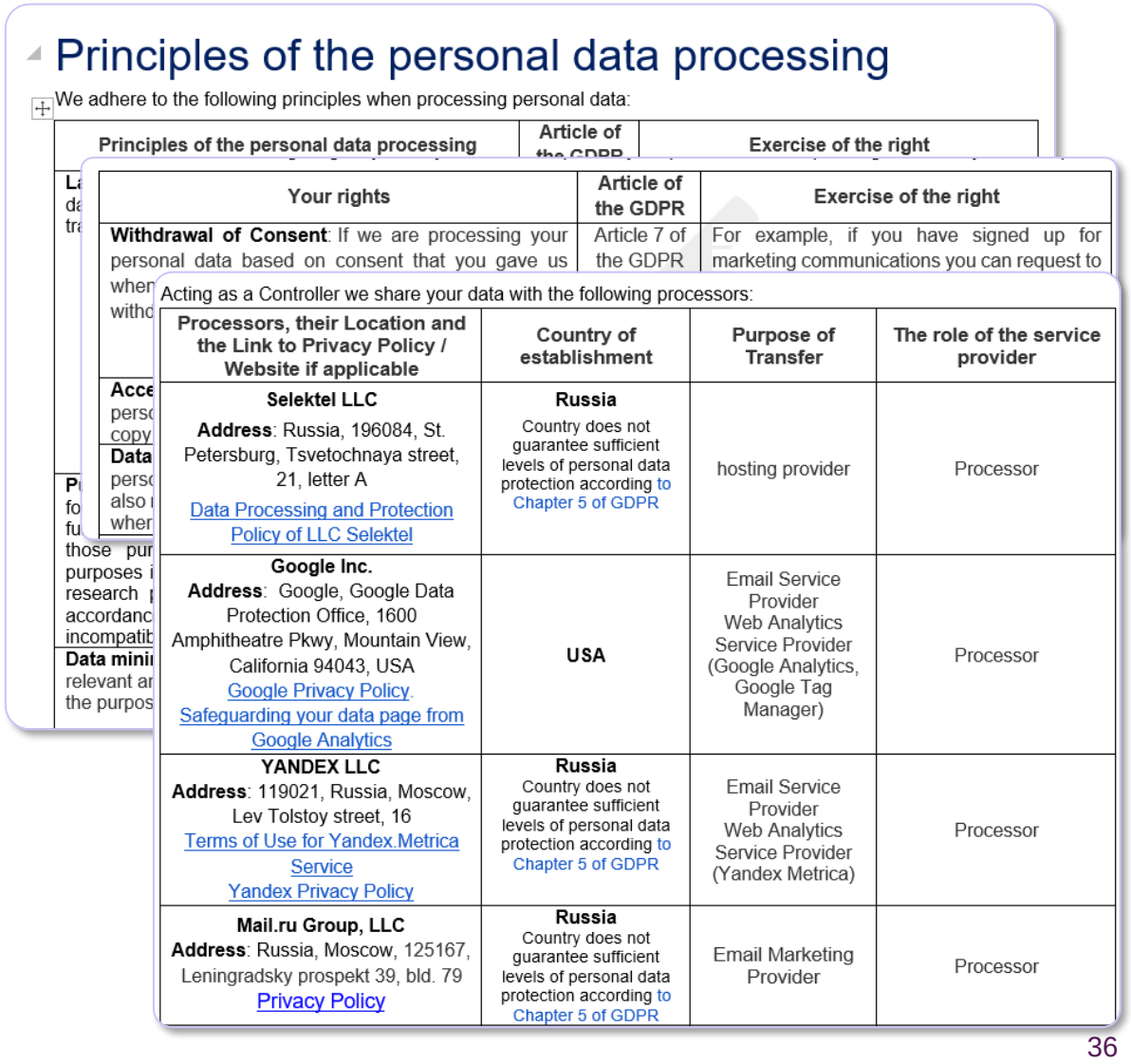
Проблема:

Донесение информации о трансграничной передаче ПДн до субъекта ПДн в доступном формате и на доступном языке

Решение:

Размещение Privacy Policy на онлайн-ресурсах компаний Группы. Субъект ПДн должен иметь возможность ознакомиться по крайней мере со следующей информацией:

- Принципы обработки ПДн;
- Права субъектов ПДн;
- Информация о трансграничной передаче ПДн субъектов, включая:
  - информацию о компании, которой передаются ПДн (адрес регистрации, роль в процессе);
  - объем передаваемых ПДн;
  - правовые основания передачи ПДн;
  - меры защиты, обеспечивающиеся при передаче ПДн



Principles of the personal data processing

We adhere to the following principles when processing personal data:

Principles of the personal data processing	Article of the GDPR	Exercise of the right

Your rights	Article of the GDPR	Exercise of the right
Withdrawal of Consent: If we are processing your personal data based on consent that you gave us	Article 7 of the GDPR	For example, if you have signed up for marketing communications you can request to

Acting as a Controller we share your data with the following processors:

Processors, their Location and the Link to Privacy Policy / Website if applicable	Country of establishment	Purpose of Transfer	The role of the service provider
Selektel LLC **Address**: Russia, 196084, St. Petersburg, Tsvetochnaya street, 21, letter A Data Processing and Protection Policy of LLC Selektel	**Russia** Country does not guarantee sufficient levels of personal data protection according to Chapter 5 of GDPR	hosting provider	Processor
Google Inc. **Address**: Google, Google Data Protection Office, 1600 Amphitheatre Pkwy, Mountain View, California 94043, USA Google Privacy Policy. Safeguarding your data page from Google Analytics	**USA**	Email Service Provider Web Analytics Service Provider (Google Analytics, Google Tag Manager)	Processor
YANDEX LLC **Address**: 119021, Russia, Moscow, Lev Tolstoy street, 16 Terms of Use for Yandex.Metrica Service Yandex Privacy Policy	**Russia** Country does not guarantee sufficient levels of personal data protection according to Chapter 5 of GDPR	Email Service Provider Web Analytics Service Provider (Yandex Metrica)	Processor
Mail.ru Group, LLC **Address**: Russia, Moscow, 125167, Leningradsky prospekt 39, bld. 79 Privacy Policy	**Russia** Country does not guarantee sufficient levels of personal data protection according to Chapter 5 of GDPR	Email Marketing Provider	Processor

Соответствие требованиям законодательства при трансграничной передаче ПДн

- Инвентаризация процессов, в рамках которых происходит передача ПДн
- Определение требований применимого законодательства при передаче ПДн
- Определение используемых инструментов передачи ПДн
- Проведение оценки воздействия передачи ПДн на субъекта ПДн при трансграничной передаче ПДн (TIA)
- Доведение информации об осуществлении трансграничной передачи ПДн до субъектов ПДн

Контакты

cyber@kept.ru

www.kept.ru