

# АЛРУД

[alrud.com](http://alrud.com)



# Как гармонично соблюсти GDPR и российское законодательство в сфере защиты персональных данных

12 июля 2018 года

[alrud.com](http://alrud.com)



|| Часть 1. Тест  
применимости  
Регламента

# Тест 1. Обработка в контексте деятельности учреждения в ЕС

Обрабатываются ли Персональные данные **Субъектов**, которые физически находятся **в Европейском Союзе**?

---

**Да**

Регламент **применяется**

---

**Нет**

Регламент **не применяется**

---

## Тест 2. Обработка в контексте предложения товаров или услуг без учреждения в ЕС

Предлагаются ли **товары или услуги** Субъектам персональных данных **в Европейском Союзе**?

---

**Да**

Регламент **применяется**

---

**Нет**

Регламент **не применяется**

---

# Тест 3. Мониторинг деятельности субъектов в ЕС независимо от наличия учреждения

Осуществляется ли **мониторинг** поведения **в Европейском Союзе**?

---

**Да**

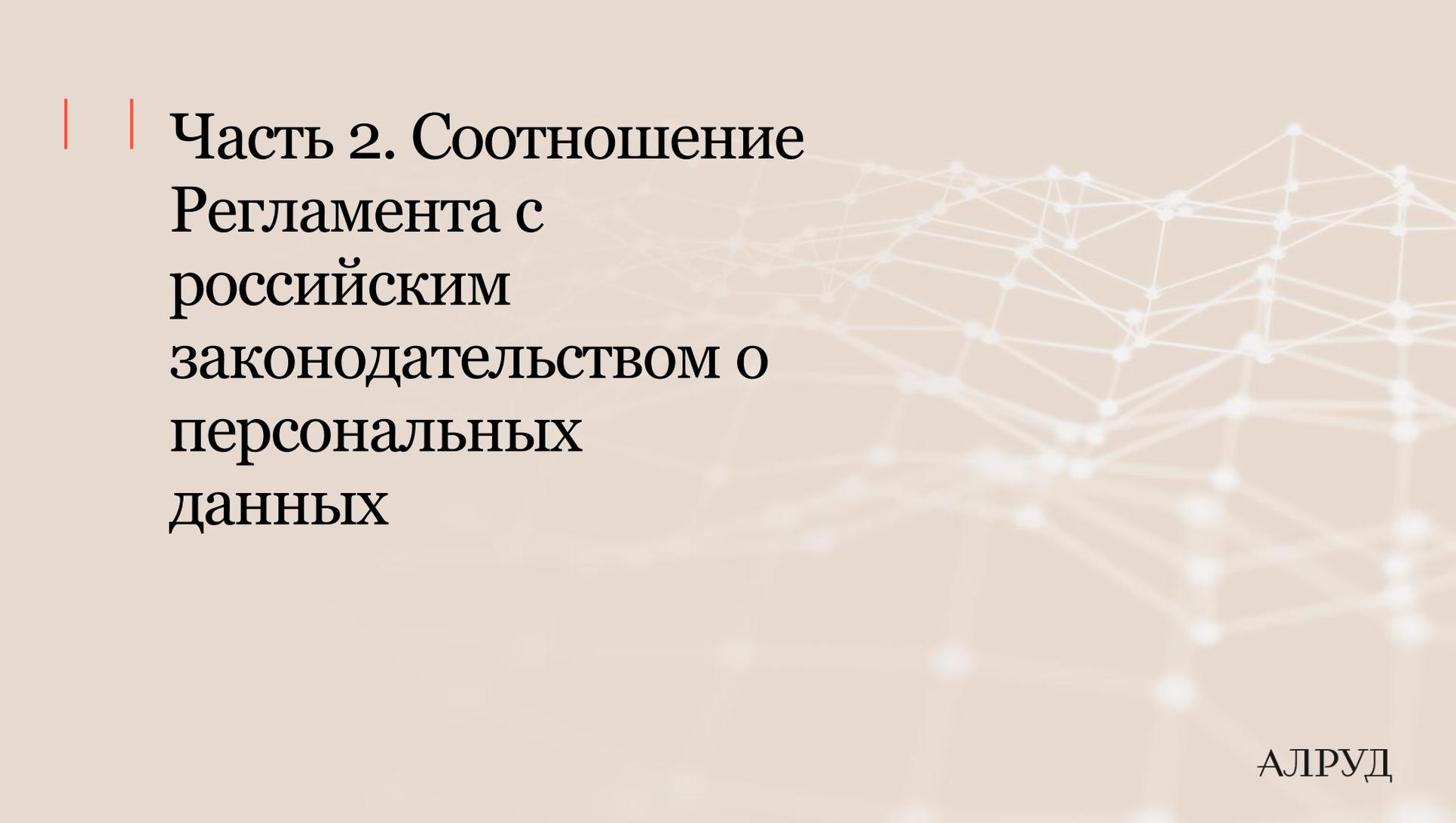
Регламент **применяется**

---

**Нет**

Регламент **не применяется**

---



Часть 2. Соотношение  
Регламента с  
российским  
законодательством о  
персональных  
данных

# ЕС и РФ: общие принципы



Законная и справедливая основа обработки



Ограниченность целями обработки

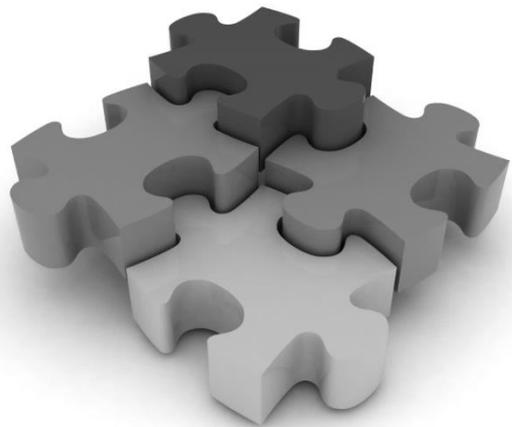


Точность, достаточность и актуальность  
персональных данных



Конфиденциальность и безопасность  
обрабатываемых персональных данных

# ЕС и РФ: сходства



- Базовые права субъектов ПДн
- Принятие мер защиты ПДн
- Оценка вреда и уровня защищенности
- Принцип минимизации обработки (ограниченность достижением цели, установленных сроков обработки)

# РФ и ЕС: отличия (1)

- Законные основания для обработки: широкое применение законного интереса в ЕС vs широкое применение согласия в РФ
- Трансграничная передача ПДн
- Обработка ПДн обработчиками
- Персональные данные детей



## РФ и ЕС: отличия (2)



- Подход к правам субъектов ПДн
- Подход к обезличенным данным
- Назначение DPO
- Регистрация в надзорном органе VS Records of processing activities
- 72 часа на уведомление о нарушении

# Законный интерес

- Обработка является законной, если она **«необходима для осуществления законных интересов»**, за исключением случаев, когда такие интересы пересекаются с интересами или основными правами и свободами субъекта ПДн
- Необходим тест на баланс интересов



# Тест на баланс интересов

Следующие цели могут считаться законным интересом:

- Предотвращение мошенничества
- Внутреннее управление
- Обеспечение безопасности сети и информации
- Экономические интересы оператора, если нет чрезмерного вмешательства в интересы, права и свободы субъекта ПДн



# Пример законного интереса

- Рассылка информации маркетингового характера получателям, которые ранее заказывали аналогичные товары или услуги и / или находятся в процессе исполнения договорных отношений с оператором **не требует согласия по GDPR**
- ФЗ РФ «О персональных данных» требует всегда получать предварительное согласие на прямую маркетинговую коммуникацию



# Унификация системы защиты

<b>GDPR</b>	<b>Россия</b>	<b>Что это значит?</b>
Data mapping	Аудит процессов	Понимание всех процессов обработки
Privacy by design	Модель угроз, оценка уровней защищенности	Оценка рисков и определение адекватных мер защиты
Impact assessment	Оценка вреда	Оценка вреда, который может быть причинен субъектам и определение адекватных мер

# Унификация системы защиты

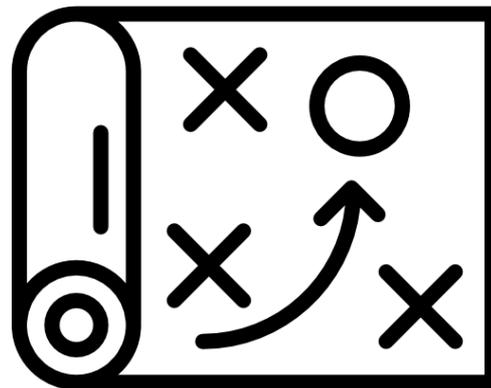
<b>GDPR</b>	<b>Россия</b>	<b>Что это значит?</b>
Privacy by default	Ограничение процессов обработки	Использование технологий по умолчанию, ограничивающих процессы обработки заявленными целями и сроками
Implementation	Организация системы защиты данных	Применение комплекса организационных, юридических и технических мер (политики, шифрование, разграничение доступа и т.д.)



# Заключительные выводы

# Предварительные действия

- Получение заключения зарекомендовавшей себя юридической фирмы о применимости Регламента к компании
- Разработка стратегии по внедрению требований Регламента



# ВЫЗОВЫ

- Неопределенные сроки хранения (большинство ИС в бизнесе)
- *Privacy by design* – учитывать требования законодательства о ПДн на всем жизненном цикле информации
- Определить «*надлежащие*» меры безопасности
- Более строгие договорные обязательства со стороны операторов <=> требования к выбору обработчиков

# Что дальше?

Совет Европы принял **поправки** к Конвенции о защите персональных данных № 108



Новые положения во многом **соответствуют** требованиям Регламента



Требования Регламента в любом случае станут **обязательными?**

alrud.com

## Контакты:



Анастасия Петрова  
Консультант

APetrova@alrud.com

ALRUD Law Firm

ул. Скаковая, д. 17, стр. 2, 6 эт.

Москва, Россия, 125040

T: +7 495 234 96 92

F: +7 495 956 37 18

E: info@alrud.com

АЛРУД