

Методика оценки применимости GDPR в отношении процессов обработки персональных данных

Перечень применённых в документе сокращений и их расшифровки

Сокращение	Расшифровка
ПД	Персональные данные
GDPR	General Data Protection Regulation (Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС)
EDPB	European Data Protection Board (Европейский совет по защите данных)
EEA	European Economic Area (Европейская экономическая зона) ¹
exp.	Обозначение примера (Example), иллюстрирующего ситуацию
гс.	Обозначение номера пункта (Recital) из преамбулы к GDPR

Территориальная сфера применения непосредственно закреплена в ст.3 GDPR и ограничивается пределами EEA, однако действие GDPR распространяется на контролёров (controller) и обработчиков (processor), находящихся за пределами EEA. В целях обеспечения того, чтобы физические лица не были лишены защиты, на которую они имеют право в соответствии с GDPR, обработка ПД субъектов в EEA контролёром или обработчиком, которые не учреждены в EEA, подпадает под действие GDPR в случаях, когда:

1. обработка ПД осуществляется в контексте деятельности учреждения контролёра или процессора, которое расположено на территории EEA;
2. обработка ПД субъектов ПД, находящихся на территории EEA, осуществляется контролёром или процессором, учрежденным за пределами EEA, и такая обработка ПД связана с:
 - a) предложением товаров или услуг указанным субъектам ПД, или
 - b) осуществлением мониторинга поведения таких субъектов ПД на территории EEA.
3. обработка ПД субъектов ПД, находящихся на территории EEA, осуществляется контролёром, учрежденным за пределами EEA в случаях, когда законодательство применяется на основании публичного международного права (дипломатические представительства, консульства).

Предложение товаров и услуг, подпадающее под действие GDPR:

1. предложение товаров и услуг направлено на субъектов EEA (наличие веб-сайта на языке стран EEA, возможность оплаты в валюте стран EEA);
2. наличие рекламных кампаний, направленных на аудиторию стран EEA;
3. международный характер деятельности (например, транспорт, туризм, банковская деятельность, гостиничный бизнес, телеком, страхование);
4. использование доменного имени верхнего уровня, отличного от страны, в которой предлагаются товары или услуги (например, .com, .eu);
5. наличие информации о получении товаров и услуг для субъектов EEA;
6. упоминание о наличии международных клиентов (клиенты из стран EEA);
7. осуществление доставки в страны EEA.

Осуществление мониторинга поведения, подпадающее под действие GDPR:

1. наличие таргетированной рекламы;
2. отслеживание местоположения, в частности, для маркетинговых целей;
3. использование файлов cookie, IP-адресов и других средств в целях профилирования пользователей;
4. персонализированные услуги по анализу состояния здоровья и питания (например, приложение, позволяющее отслеживать состояние здоровья);
5. обследование рынка и другие поведенческие исследования на основе индивидуальных профилей.

Также следует обратить внимание на необходимость дополнительной верификации признаков применимости норм GDPR с помощью следующих документов EDPB регуляторного характера:

1. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3);
2. Guidelines 5/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

Таким образом, определение наличия признаков применимости норм GDPR в отношении тех или иных процессов обработки ПД организации может быть выполнено посредством последовательного выбора ответов на вопросы закрытого типа (см. Перечень вопросов и Блок-схему) для получения вывода о наличии признаков применимости норм GDPR.

Не следует абсолютизировать эффективность описанной выше методики оценки применимости GDPR в отношении обработки ПД, так как суды EEA не обязаны следовать толкованию норм GDPR со стороны EDPB и национальных надзорных органов. Так, в п.55 решения² Royal Court of Justice (г. Лондон, Великобритания) от 15.01.2021г. по делу QB-2020-002450 в части территориальной применимости GDPR был указано, что EDPB Guidelines 3/2018 приняты судом во внимание, являются «убедительными, но не обязательными» (*are persuasive, not binding*).

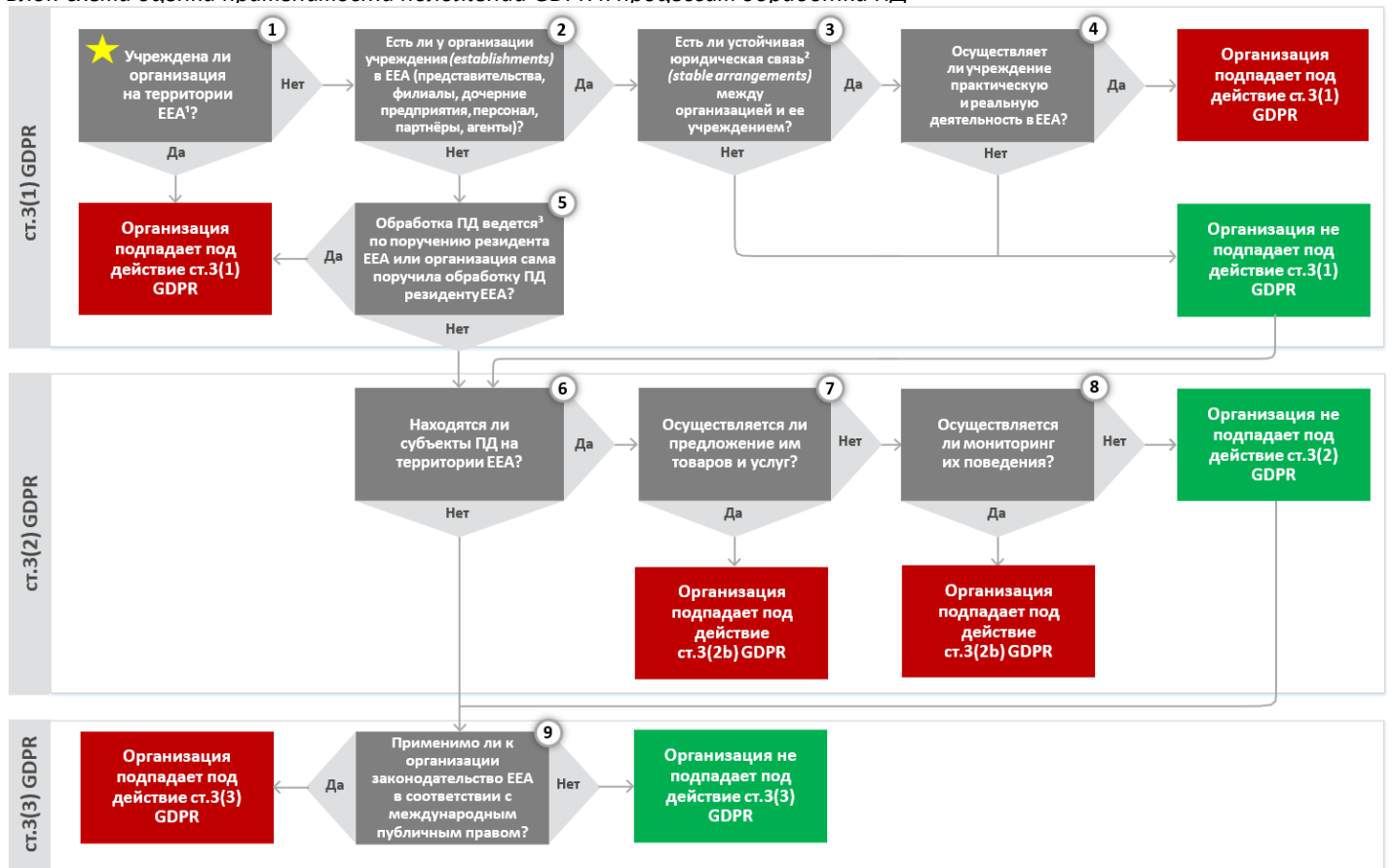
¹ Используется для обозначения стран, в которых применяются нормы GDPR – государства-члены Европейского Союза и некоторые государства-члены Европейской ассоциации свободной торговли (Норвегия, Исландия и Лихтенштейн). Великобритания и Швейцария формально не являются государствами-членами EEA, и в указанных странах нормы GDPR прямо не применяются, хотя национальное законодательство этих стран о ПД в максимальной степени гармонизировано с положениями GDPR.

² См. <https://www.bailii.org/ew/cases/EWHC/QB/2021/56.pdf>

Перечень вопросов для оценки применимости положений GDPR к процессам обработки ПД

№	Вопрос	Ответ	GDPR	3/2018	5/2021
1	Учреждена ли организация на территории ЕЕА?	Да – GDPR применим Нет – см. вопрос 2	ст.3(1) rc.22	п.1(a) exp.1	п.13,16,18 exp.3-4, 6-7
2	Есть ли у организации учреждения (establishments) в ЕЕА (представительства, филиалы, дочерние предприятия, персонал, партнёры, агенты)?	Да – см. вопрос 3 Нет – см. вопрос 5			
3	Есть ли устойчивая юридическая связь ³ (stable arrangements) между организацией и ее учреждением?	Да – см. вопрос 4 Нет – см. вопрос 6			
4	Осуществляет ли учреждение практическую и реальную деятельность в ЕЕА?	Да – GDPR применим Нет – см. вопрос 6			
5	Обработка ПД ведется ⁴ по поручению резидента ЕЕА или организация сама поручила обработку ПД резиденту ЕЕА?	Да – GDPR применим Нет – см. вопрос 6			
6	Находятся ли субъекты ПД на территории ЕЕА?	Да – см. вопрос 7 Нет – см. вопрос 9	ст.3(2) rc.14	п.2(a) exp.8-12	п.18 exp.7
7	Осуществляется ли предложение товаров и услуг субъектам ПД на территории ЕЕА?	Да – GDPR применим Нет – см. вопрос 8	ст.3(2a) rc.23	п.2(b) exp.13-16	
8	Осуществляется ли мониторинг поведения субъектов ПД на территории ЕЕА?	Да – GDPR применим Нет – см. вопрос 9	ст.3(2b) rc.24	п.2(c),(d) exp.17-21	
9	Применимо ли к организации законодательство ЕЕА согласно международному публичному праву?	Да – GDPR применим Нет – GDPR не применим	ст.3(3) rc.25	п.3 exp.22-23	–

Блок-схема оценки применимости положений GDPR к процессам обработки ПД



³ Наличие правоотношений, вне зависимости от их формы (соглашения, контракты, участие в уставном капитале и т.д.).

⁴ Обработка ПД, выполняемая на основании и для исполнения договора между оператором и обработчиком (Controller-to-Processor Agreement), ведется в контексте практической и реальной деятельности организации, находящейся в статусе оператора или обработчика, на территории ЕЕА. Применимость GDPR определяется отдельно для каждого факта поручения обработки ПД и не зависит от места фактического осуществления обработки ПД (на территории ЕЕА или вне неё).