Сравнительный анализ GDPR и Российского законодательства

Дата доклада: 20.09.2018
Докладчик: Калашникова Е.В.
Заместитель начальника Управления по обеспечению информационной безопасности — руководитель службы,
Банк ВТБ (ПАО)

General Data Protection Regulation - GDPR

Вступил в силу	25 мая 2018 г.
Содержание	173 пункта преамбулы, 11 глав, 99 статей.
Отменяет	Директиву 95/46/EC.
Применимость в РФ	Открытый вопрос.

Основные понятия (Глава 1 статья 4 GDPR)

GDPR	*152-ФЗ*
Персональные данные	С учетом разъяснений, даваемых представителями регуляторов (например, интервью А. Жарова в 2013г.) и судебной практики (например, Решение Арбитражного суда г. Москвы от 11.03.2016 по делу № А40-14902/2016) – аналогично.
Псевдонимизация	Обезличивание.
Контролер	Оператор.
Обработчик	Лицо, указанное в части 3 статьи 6 152-ФЗ.
Получатель	Нет специального термина.
Биометрические данные	Изображение лица в некоторых случаях исключается (пример: Разъяснения Роскомнадзора от 30.08.2013г. «Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки»).

Выводы:
В основном понятийный аппарат совпадает. В GDPR определен ряд терминов (например, «третье лицо», «согласие», «данные о здоровье», которым в 152-ФЗ просто не уделено внимание и они употребляются в общепринятом смысле).

Кстати, определение «данных о здоровье» из GDPR так же не исключает различных трактовок данного понятия.

Принципы (Глава 2 GDPR)

GDPR	*152-ФЗ*
Принципы обработки	Совпадают.
Подотчетность	Фактически, данный принцип установлен уполномоченными законом регуляторами.
Правомерность обработки	Совпадают. В 152-ФЗ некоторые основания изложены подробнее.
Согласие на обработку	Существенные условия совпадают. 152-ФЗ не акцентирует отдельно внимание на процедурах получения согласия несовершеннолетнего, но данный случай по законодательству соответствует положениям о возможности законному представителю выступать от имени субъекта ПДн.
Обработка особых категорий ПДн	Условия совпадают, но 152-ФЗ требует письменного согласия, GDPR – явного.
Общедоступные ПДн	В отличие от GDPR, 152-ФЗ требует письменного, а не просто явного согласия на включение данных в общедоступные источники.
Обработка без идентификации	Не противоречит, но отдельно не упоминается.

Выводы:

Основные принципы обработки ПДн совпадают. GDPR в отличие от 152-ФЗ не предъявляет жестких требований по получению письменного согласия на обработку, например, биометрических ПДн или помещения персональных данных в общедоступные источники, достаточно, чтобы согласие было явным и дано в доказуемой форме.

Права субъекта персональных данных (Глава 3 GDPR)

GDPR	*152-ФЗ*
Прозрачность	Также обязывает Оператора предоставлять информацию об обработке данных.
Предоставляемая информация	В обоих случаях субъект ПДн может получить одинаковый объем информации. Только по GDPR Контролер обязан предоставить эту информацию при сборе данных, а по 152-ФЗ Оператор предоставляет ее по запросу. При этом GDPR предусматривает исключение из этой обязанности (когда указанная обязанность делает невозможным или негативно отражается на достижении целей обработки).
Доступ к ПДн	Совпадает.
Исправление данных	Совпадает. В 152-ФЗ изложено с позиции обязанности Оператора.
Право на забвение	В терминологии 152-ФЗ – удаление. Дополнительно в РФ введен Федеральный закон от 13 июля 2015 г. N 264-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации (поисковые системы).
Ограничение обработки ПДн	В полном объеме не выделено явно. Есть понятие блокировки.
Уведомление при изменении	Такая обязанность Оператора явно не предусмотрена.
Ограничения на уровне государства	Не применимо, поскольку закон федеральный.

Выводы:

Основные права субъектов ПДн совпадают. GDPR с одной стороны в явном виде накладывает на Контролера больше обязательств, чем 152-ФЗ, но и шире трактует возможности отступления от правил.

Контролер и обработчик (Глава 4 GDPR, раздел 1)

GDPR	*152-ФЗ*
Ответственность Контролера	В целом совпадает, однако GDPR вводит понятие соизмеримости мер защиты к обработке данных.
Минимизация обрабатываемых ПДн	Совпадает.
Сертификация	GDPR предусматривает возможность добровольной сертификации соответствия защиты данных установленным требованиям на срок до 3 лет с возможностью продления сертификата. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных“ устанавливает необходимость проверки 1 раз в 3 года, однако аттестация систем является обязательной только для первого уровня защищенности ПДн.
Действующие совместно Контролеры	В GDPR в явном виде указано, что Контролеры могут действовать совместно. Однако никаких преимуществ им это не дает, субъект ПДн имеет право действовать в отношении каждого из Контролеров отдельно. 152-ФЗ не выделяет особо такую конструкцию, тем не менее, механизм поручения обработки ПДн предусмотрен.
Представитель Контролера в ЕС	В GDPR не применяется если не охватывает больших объемов особых категорий ПДн, данных об уголовных правонарушениях, и едва ли может повлечь за собой риски правам и свободам субъектов ПДн. К 152-ФЗ не применимо, поскольку закон федеральный.
Обработчик	Не противоречит. Менее детально, но по существу аналогично тому, что указано для лица, которому поручается обработка ПДн.
Сотрудничество с надзорным органом	Предусмотрен уполномоченный орган, о сотрудничестве явно не указано, но есть более жесткие требования.

Выводы:

Основные положения совпадают. GDPR предполагает добровольную сертификацию, ФСТЭК России (17 Приказ) требует аттестацию только для государственных ИСПДн.

Безопасность персональных данных (Глава 4 GDPR, раздел 2)

GDPR	*152-ФЗ, 1119-ПП, СТО БР ИББС-1.0-2014, ГОСТ Р 57580.1-2017, 17 и 21 приказы ФСТЭК*
Псевдонимизация	Обезличивание, там, где это возможно. Пример – требования СТО БР ИББС-1.0-2014 и ГОСТ Р 57580.1-2017, запрещающие использовать реальные данные в тестовых средах (не только ПДн).
Криптографическая защита	В GDPR нет требований к сертификации СКЗИ. В РФ с учетом п. 2 «Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденных руководством 8 Центра ФСБ России 31.03.2015г. № 149/7/2/6-432 и Положения об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, утвержденным постановлением Правительства Российской Федерации от 15.05.2010г. № 330, использование сертифицированных СКЗИ для защиты ПДн при передаче по каналам связи, выходящим за границу КЗ, является обязательным. Для СКЗИ в ИСПДн СТО БР ИББС-1.0-2014 требует класс не ниже КС2.
Средства обеспечения постоянной Ц, Д, К, У	Предусмотрено СТО БР ИББС-1.0-2014, ГОСТ Р 57580.1-2017, 17 и 21 приказами ФСТЭК.
Восстановление после инцидентов	Планы ОНиВД в соответствии с Положением Банка России от 16 декабря 2003 г. N 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах».
Проверка и оценка	Не реже, чем 1 раз в 3 года (ФСТЭК), в составе СТО БР ИББС-1.0-2014 (ЦБ РФ) – 1 раз в 2 года.
Уведомление об инциденте	По GDPR – 72 часа на уведомление регулятора, в т.ч поэтапно, для субъекта срок не указан. Необходимо кроме случаев, когда утечка вряд ли обернется рисками для прав и свобод физических лиц. По 152-ФЗ не предусмотрено.

Выводы:

GDPR требует принимать меры защиты, обеспечивающие надлежащий уровень безопасности, соразмерный имеющимся рискам. Поскольку не сказано, что считать соразмерным и как оценивать, сложно сказать, насколько эти меры обязательны.

Оценка воздействия и консультация (Глава 4 GDPR, раздел 3)

GDPR	*152-ФЗ, 1119-ПП, СТО БР ИББС-1.0-2014, ГОСТ Р 57580.1-2017, 17 и 21 приказы ФСТЭК*
Оценка воздействия	1119-ПП предусматривает моделирование угроз ИБ ПДн.
Предварительная консультация	В GDPR если выявлены высокие риски, необходима предварительная консультация с надзорным органом. В РФ упразднена необходимость согласовывать модель угроз ИБ ПДн с регуляторами.

Выводы:
GDPR и российские нормативно-методические документы по данному вопросу существенно не различаются.

Инспектор по защите ПДн (Глава 4 GDPR, раздел 4)

GDPR	*152-ФЗ*
Назначение	По GDPR необходимо не во всех случаях (гос. организация, специальные категории ПДн, систематический мониторинг данных). По 152-ФЗ ответственный за организацию обработки ПДн требуется всегда.
Описание должности	GDPR выдвигает требования к наличию определенной квалификации и назначения не менее чем на 2 года. 152-ФЗ таких требований не предъявляет.
Задачи	Совпадает.

Выводы:

Основные положения совпадают. GDPR не во всех случаях требует назначения такого лица.

Трансграничная передача данных (Глава 5 GDPR)

GDPR	*152-ФЗ*
Достаточность мер	Совпадает. Предусмотрена возможность трансграничной передачи ПДн без согласия субъекта в страны, ратифицировавшие Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных.
Надлежащие гарантии	Предусмотрена возможность трансграничной передачи ПДн без согласия субъекта в страны, входящие в список обеспечивающих адекватную защиту ПДн (формирует Роскомнадзор)
Корпоративные правила	Отраслевое регулирование также допускается. Пример – СТО БР ИББС-1.0-2014.
Согласно праву	Совпадает. Передача в рамках законодательства и международных соглашений.
Изъятие в отдельных случаях	GDPR допускает еще ряд исключений, позволяющих трансграничную передачу ПДн без согласия субъекта. Есть и размытые формулировки (веские причины общественного интереса).
Международное сотрудничество	Допускается в рамках законодательства и международных соглашений.

Выводы:
Принципы организации трансграничной передачи данных совпадают.

Самостоятельные надзорные органы (Глава 6 GDPR)

К 152-ФЗ не применимо.
Уполномоченные органы устанавливаются законами и подзаконными актами в явном виде.

Иные положения (Главы 8-11 GDPR)

GDPR	*152-ФЗ*
Средства правовой защиты, ответственность и санкции	Права субъекта ПДн описаны в 152-ФЗ. Все другие права гражданина так же действуют. Ответственность и санкции определяются КоАП и др. аналогичными документами.
Вопросы, вынесенные отдельно	Есть аналогичный в чем-то механизм трактовки в виде Разъяснений уполномоченных органов и решений Верховного суда.
Подзаконные акты	Есть ссылки из закона на документы, которые должны быть разработаны уполномоченными органами.
Соотнесение с другими документами	В случае 152-ФЗ с нормативными актами Российской Федерации.

Что необходимо сделать согласно GDPR, если 152-ФЗ уже выполняется?

- ✓ Определить необходимость назначения Data Protection Officer (DPO, статья 29), при необходимости - обеспечить соответствие назначенного лица (в рамках 152-ФЗ) квалификационным требованиям, или назначить второе лицо именно под GDPR.
- ✓ Определить необходимость назначения представителя в ЕС, если обрабатываются большие объемы данных, специальные категории и в иных случаях, указанных в статье 27.
- ✓ Определить необходимость проведения оценки воздействия на конфиденциальность (статья 36).
- ✓ Предусмотреть на сайте Оператора максимальные возможности для пользователя по обращению к оператору, в т.ч. для изменения своих данных и т.д., идентификации субъекта с использованием электронных средств, получения информации об обработке его ПДн в т.ч. с использованием стандартных кнопок.
- ✓ Изложить политику в отношение обработки ПДн максимально простым и понятным языком.
- ✓ Обеспечить переносимость персональных данных (передачи от одного оператора к другому на носителе).
- ✓ Обеспечить уведомление регулятора о критичных утечках ПДн в течение 72 часов хотя бы частями, и своевременное уведомление субъекта ПДн.
- ✓ Проверить форму согласия на обработку на соответствие статьям 7 и 8.

Спасибо!

Вопросы?