GDPR, биометрическая идентификация, предоставление сведений о пользователях конечного оборудования связи – изменения законодательства о персональных данных

Емельянников
Михаил Юрьевич,
Управляющий партнер

Конференция «Информационная безопасность финансовой сферы»
20 сентября 2018 года

Главные события 2018 года

25 мая – вступление в силу на территории Евросоюза Регламента (ЕС) 2016/679 Европейского Парламента и Совета от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и свободном перемещении таких данных (General Data Protection Regulation, **GDPR**).

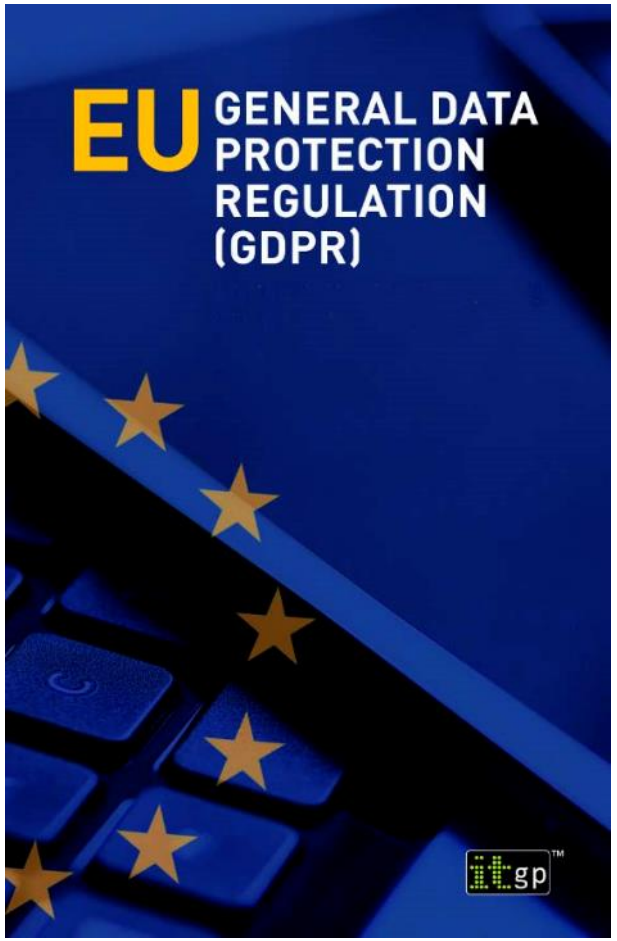
30 июня – начало функционирования системы идентификации граждан РФ на основе **биометрических персональных данных.**

1 июня - вступление в силу изменения в ФЗ «О связи», обязывающий операторов сотовой связи дополнительно проверять **достоверность** предоставленных при заключении договора клиентом сведений о себе.

GDPR – главное событие года

Регламент (ЕС) 2016/679 Европейского Парламента и Совета от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и свободном перемещении таких данных, аннулирующий Директиву 95/46/ЕС

- Унификация законов по защите персональных данных, принятых в странах ЕС
- Обеспечения высокого, единообразного и одинакового уровня защиты физических лиц во всех государствах-членах ЕС
- Защита персональных данных и расширение прав на конфиденциальность всех субъектов персональных данных в ЕС



Кому это надо знать в России?

- **Дочерним и зависимым обществам** российских компаний, работающим в ЕС
- Российским компаниям, предлагающим физическим лицам в ЕС **товары и услуги**
- Российским компаниям, осуществляющим **мониторинг** действий лиц на территории ЕС
- Российским компаниям, которым контролеры (операторы) ЕС **передали персональные данные** для обработки (хостинг, резервное копирование, статистическая обработка и т.д.)

Что это означает на практике?

Российские компании, которым ДЗК передали персональные данные лиц на территории ЕС для обработки (хостинг, резервное копирование, единые информационные системы банковских групп и банковских холдингов компаний и т.д.)

Что это означает на практике?

Мониторинг поведения клиентов российских банков при их нахождении в Евросоюзе (использование платежных карт, фрод-мониторинг, использование систем ДБО, «Клиент-банк» и др.)

Что это означает на практике?

Мониторинг поведения посетителей сайта, находящихся в Евросоюзе (IP-адреса) и использующих файлы cookie на сайтах российских операторов

Мониторинг поведения

Чтобы определить, можно ли рассматривать деятельность по обработке данных как мониторинг поведения субъектов данных, необходимо удостовериться, происходит ли отслеживание их поведения в Интернете, включая возможное последующее использование методик обработки персональных данных, которые заключаются в создании **профиля физического лица**, в особенности с целью принятия касающихся его решений или анализа и предсказания его личных предпочтений, поведения и отношений.

Идентификация с использованием биометрических данных

Обязанность банков, соответствующих критериям Банка России, проводить **первичную биометрическую идентификацию** с созданием учетной записи в ЕСИА и размещением биометрических персональных данных в ЕБС.

Обязанность предоставлять **банковские услуги** (открытие и ведение счета (вклада) клиентов - физических лиц, предоставление кредитов, переводы денежных средств по таким счетам) **без личного присутствия** клиентов – физических лиц после проведения их идентификации путем установления и подтверждения достоверности сведений о них с использованием ЕСИА и ЕБС.

Перечень банков, соответствующих требованиям

Перечень

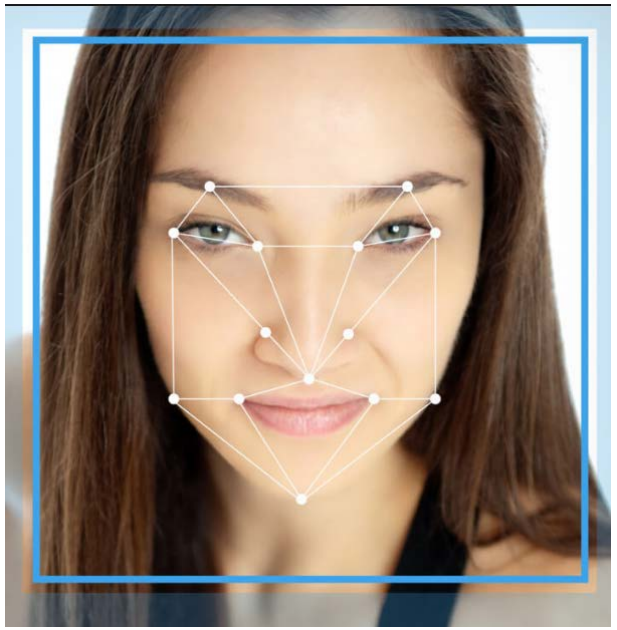
банков, соответствующих требованиям, установленным абзацами вторым - четвертым пункта 5.7 статьи 7 Федерального закона от 07.08.2001 № 115-ФЗ"О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма",

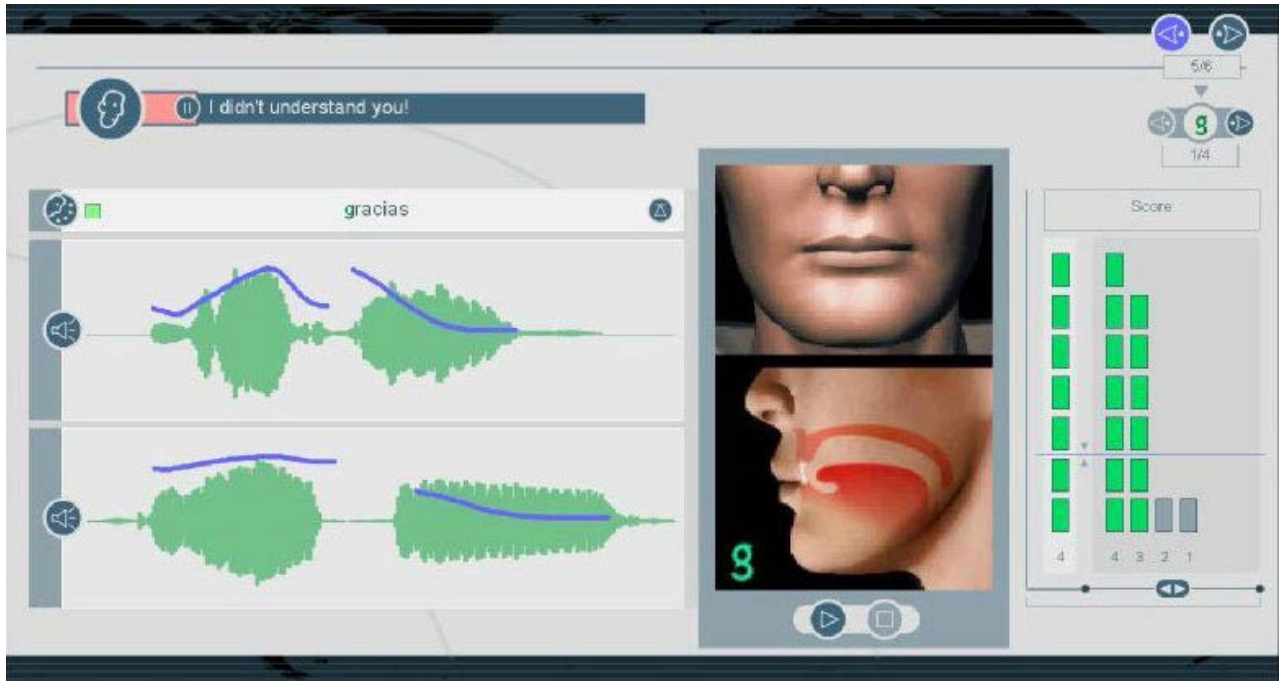
по состоянию на 30.08.2018

№ п/п	Наименование банка	Рег.№
1	АО ЮниКредит Банк	1
2	АО "КАБ "Викинг"	2
3	ООО "Примтеркомбанк"	21
...	...	...
425	ООО "Чайна Констракшн Банк"	3515
426	ООО "ОНЕЙ БАНК"	3516
427	ООО "Икано Банк"	3519
428	АО "Банк ЧБРР"	3527
429	АО "Севастопольский Морской банк"	3528

Состав обрабатываемых в ЕБС биометрических данных

- данные **изображения лица**, полученные с помощью фото- видео устройств
- данные **голоса**, полученные с помощью звукозаписывающих устройств



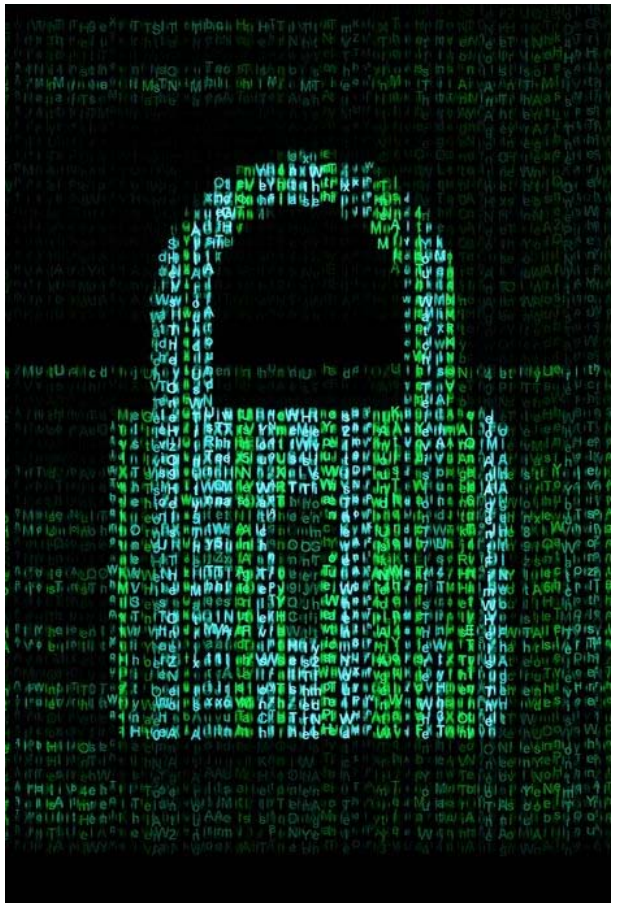


Важные особенности биометрической идентификации

- Биометрические данные хранятся не менее 50 лет.
- Согласие на их обработку дается на срок не более 50 лет.
- Данные могут использоваться для идентификации не более трех лет с даты их внесения в ЕБС.
- Отзыв согласия не влечет уничтожения или удаления данных из ЕБС, а означает лишь невозможность их использования для идентификации.
- Для сбора биометрических данных должны использоваться информационные технологии и технические средства, соответствующие требованиям Минкомсвязи России.
- Вероятность соответствия биометрических данных должна быть не менее 0,9999.
- Банк России может ввести лимиты по количеству открытых счетов, размеру кредита и сумме перевода денежных средств.

Использование СКЗИ при биометрической идентификации

- КС-1 – в канале клиент-банк при удаленной идентификации
- КС-2 или КС-3 – при передаче между структурными подразделениями банка
- КВ – в канале между банком и ЕБС
- КВ – в ЕБС



Использование СКЗИ при биометрической идентификации

В случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия посредством сети Интернет использует указанные ниже устройства:

- **мобильный телефон, смартфон или планшетный компьютер** и отказывается от использования шифровальных (криптографических) средств, банк **обязан отказать** такому лицу в проведении указанной идентификации;
- **иные устройства**, в том числе **персональный компьютер**, и отказывается от применения шифровальных (криптографических) средств, банк **уведомляет его о рисках**, связанных с таким отказом. После подтверждения физическим лицом своего решения можно провести соответствующую идентификацию физического лица посредством сети Интернет **без использования** им указанных шифровальных (криптографических) средств.

Цена вопроса

Коммерсантъ | ГАЗЕТА КОММЕРСАНТЪ 3 сентября 2018

Банки оценили биометрию. Многим она оказалась не по карману

Минимальный набор средств:

- HSM-модуль
- операционная система с заданными параметрами
- средство электронной подписи снимаемой биометрии
- антивирус
- межсетевой экран
- системы обнаружения угроз (вторжений?)

Цена подключения банка с одним отделением – от 3 млн руб.

Каждое следующее отделение – 130 тыс. руб.

Настройка оборудования, аттестация системы, разработка модели угроз и модели нарушителя, годовое обслуживание – 1,2 млн руб.

Основные проблемы биометрической идентификации

- Порядок действий при компрометации биометрических персональных данных
- Порядок оспаривания операций, совершенных с использованием биометрической идентификации
- Сроки хранения биометрических данных после их обновления и отзыва согласия на такую идентификацию
- Биометрическая идентификация не вызвана бизнес-интересами банков и может иметь далеко идущие последствия для граждан

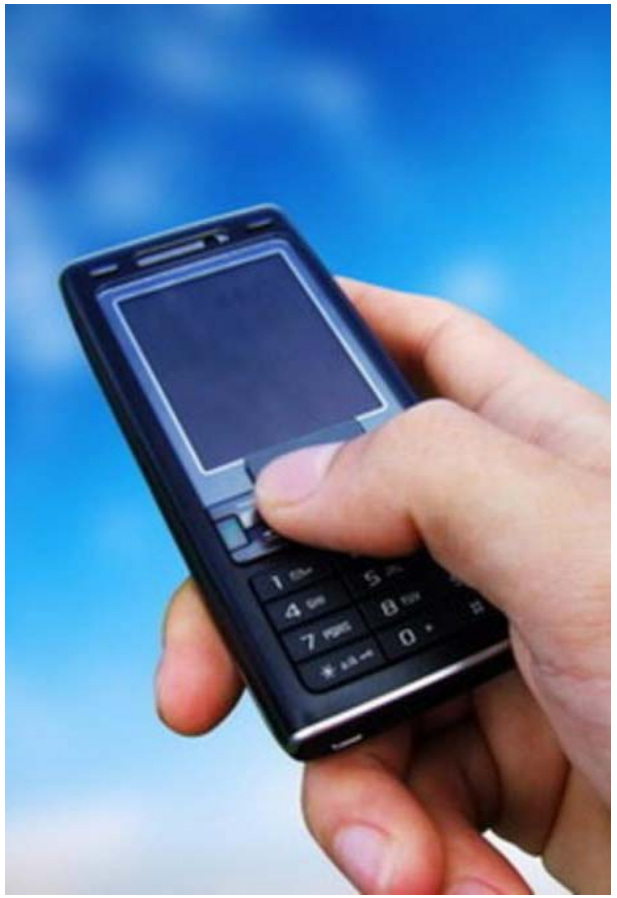
Идентификация пользователя услуг связи

Услуги сотовой связи предоставляются **абоненту** - физическому лицу, юридическому лицу либо индивидуальному предпринимателю и **пользователю услугами связи такого абонента**, достоверные сведения о которых предоставлены оператору связи в соответствии с правилами оказания услуг связи.

Абонент - юридическое лицо либо индивидуальный предприниматель обязаны предоставить оператору связи сведения о пользователях услугами связи в соответствии с правилами оказания услуг связи.

Правила оказания услуг телефонной связи

Абонент обязан **ежеквартально** представлять оператору связи заверенный надлежащим образом **список лиц, использующих оборудование абонента** – юридического лица, содержащий фамилии, имена, отчества, места жительства, реквизиты документа, удостоверяющего личность этих лиц, а в случае изменения фактических пользователей оборудования юридического лица – представлять **сведения о новых пользователях** не позднее **15 дней** со дня, когда об этом стало известно.



Правила оказания услуг телефонной связи

Оператор связи обязан при поступлении соответствующего запроса от органа, осуществляющего оперативно-розыскную деятельность, в течение 3 рабочих дней со дня получения такого запроса направить абоненту запрос с требованием подтвердить **соответствие персональных данных фактического пользователя** сведениям, заявленным в договоре, с указанием даты прекращения оказания услуг связи в случае неподтверждения соответствия персональных данных.

Спасибо!
Вопросы?

Емельянников
Михаил Юрьевич
Управляющий партнер
+7 (495) 761 5865
info@mezp.ru
http://emeliyannikov.blogspot.ru/