

20.03.2024

## Особенности правового регулирования защиты персональных данных в Международном финансовом центре “Астана”

*Екатерина Хамидуллина,*

*Партнёр Юридической фирмы «AEQUITAS»,*

*руководитель AEQUITAS AIFC Branch,*

*магистр международного бизнес-права и технологий*

В последние годы растёт интерес бизнеса, особенно иностранных инвесторов, к Международному финансовому центру “Астана” (“МФЦА”). В рамках МФЦА Казахстан впервые на постсоветском пространстве ввел специальную юрисдикцию, основанную на принципах коммерческого права Англии и Уэльса. МФЦА ставит своей целью привлечение инвестиций в экономику Казахстана, развитие местных рынков капитала и создание эффективных проектов в сфере производства товаров и услуг. По состоянию на 7 марта 2024 года в МФЦА зарегистрировано 2 608 компаний<sup>[1]</sup>.

Нормативно-правовая база МФЦА активно развивается. В настоящей статье мы рассмотрим актуальную тему, касающуюся правового регулирования защиты персональных данных в МФЦА, основу которого составляют Положение МФЦА о защите данных (далее - “Положение”)<sup>[2]</sup> и Правила защиты данных<sup>[3]</sup>. Оба акта были разработаны после принятия широко известного GDPR<sup>[4]</sup>, который многие эксперты в сфере защиты персональных данных оценивают как “золотой стандарт” или эталонную модель защиты персональных данных в Европе и за её пределами, принимая во внимание экстратерриториальный эффект действия GDPR.

Полагаем, что разработчики актов МФЦА в сфере защиты персональных данных ориентировались на модель GDPR. Положение в tandem с Правилами защиты данных можно охарактеризовать как “облегчённую”, краткую версию GDPR. Поскольку акты МФЦА кардинальным образом отличаются от Закона РК о персональных данных<sup>[5]</sup>, мы не будем приводить сравнительный анализ регулирования защиты данных в Казахстане и МФЦА, который может стать предметом нашего отдельного анализа в будущем. В данной статье будут рассмотрены ключевые моменты регулирования в МФЦА в сравнении с GDPR.

### 1. Основные понятия Положения

2.

Актами МФЦА в сфере защиты данных не предусмотрены такие привычные для казахстанского бизнеса понятия, как собственник или оператор базы, содержащей персональные данные, указанные в Законе РК о персональных данных. Вместо них, по аналогии с GDPR, Положением предусмотрены понятия “лица” (Person), “контролёра данных” (Data Controller), “обработчика данных” (Data Processor).

В рамках МФЦА под “персональными данными” понимаются любые данные, относящиеся к идентифицируемому физическому лицу (далее - “Персональные данные”). “Лицо” включает любое физическое лицо, зарегистрированную организацию или общественное объединение без образования юридического лица, в том числе компанию, товарищество, неинкорпорированную ассоциацию, правительство или государство (далее - “Лицо”).

Под контролёром данных понимается любое Лицо в МФЦА, которое самостоятельно или совместно с другими Лицами определяет цели и средства обработки Персональных данных (далее - “Контролёр”). Под обработчиком данных понимается любое Лицо, которое обрабатывает Персональные данные от имени Контролёра (далее - “Обработчик”).

“Персональные данные ограниченного доступа” (Sensitive Personal Data) включают данные, относящиеся прямо или косвенно к расовому или этническому происхождению, политическим взглядам или принадлежности, философским или религиозным убеждениям, сведениям о судимости, членству в профсоюзе, здоровью или сексуальной жизни, а также деятельности в сообществах. При этом определение понятия Персональных данных

ограниченного доступа весьма схоже с понятием специальных категорий персональных данных, предусмотренным пунктом 1 статьи 9 GDPR.

“Третья сторона” в отношении Персональных данных означает любое Лицо, кроме Субъекта данных, Контролёра, Обработчика или Лица, которое под прямым контролем Контролёра или Обработчика уполномочено обрабатывать Персональные данные (далее - “Третья сторона”).

Комиссаром по вопросам защиты данных (далее - “Комиссар”) может быть назначено квалифицированное и опытное физическое лицо, утверждённое советом директоров Администрации МФЦА после консультации с Управляющим МФЦА. К функциям Комиссара относится администрирование Положения, Правил защиты данных, предотвращение, выявление и ограничение поведения, которое может противоречить актам МФЦА в сфере защиты данных. Комиссар должен способствовать повышению осведомленности и пониманию вопросов защиты данных в МФЦА, требований Положения, Правил защиты данных и другого законодательства, администрируемого Комиссаром.

### 3. Сходство положений актов МФЦА о защите Персональных данных с GDPR

4.

Положением предусмотрены ключевые принципы обработки Персональных данных аналогичные тем, которые указаны в GDPR, включая законность, справедливость, точность, минимизацию Персональных данных, ограничение цели их обработки, безопасность и ограничение срока хранения.

Контролёр вправе обрабатывать Персональные данные ограниченного доступа, если субъект данных предоставил согласие, а также в некоторых других случаях, предусмотренных Положением. Данные случаи схожи с исключениями, предусмотренными для обработки специальных категорий персональных данных в рамках GDPR.

Контролёр должен создавать и вести записи, предусмотренные Правилами защиты данных, уведомлять Комиссара в отношении операций, относящихся к обработке Персональных данных. В свою очередь, Комиссар несет ответственность за ведение Реестра уведомлений по вышеуказанным операциям.

В GDPR предусмотрены ограничения на передачу персональных данных в страны, находящиеся вне Европейской экономической зоны (ЕЭЗ), законодательством которых не предусмотрены требования по защите данных. Согласно Положению, также не разрешается передавать Персональные данные за пределы МФЦА, если в другой юрисдикции не обеспечивается достаточный уровень их защиты. В Приложении № 2 к Правилам защиты данных приводится Перечень юрисдикций с достаточным уровнем защиты Персональных данных, который включает 32 страны, в основном расположенные в Европе.

Передача данных в юрисдикции, не обеспечивающие достаточного уровня защиты, допустима в некоторых случаях, в том числе: (i) при наличии разрешения, выданного Комиссаром; (ii) при наличии письменного согласия субъекта данных; (iii) если передача данных необходима для выполнения контракта, стороной которого является или намерен быть субъект данных; (iv) передача необходима для завершения или выполнения контракта, заключённого в интересах субъекта данных между Контролёром и Третьим лицом; (v) передача необходима для выполнения юридического обязательства, которому подчиняется Контролёр данных, или передача осуществляется по запросу регулирующего органа, полиции или другого государственного органа любой юрисдикции; (vi) передача необходима для защиты жизненно важных интересов субъекта данных и в некоторых других случаях. В целом вышеуказанные случаи схожи с аналогичными положениями, предусмотренными GDPR.

### 3. Некоторые различия в регулировании защиты Персональных данных, предусмотренные актами МФЦА и GDPR

Одной из отличительных особенностей регулирования является то, что обработка Персональных данных ограниченного доступа разрешена в МФЦА, помимо прочего, если это необходимо для обеспечения соответствия требованиям противодействия легализации отмыкания доходов, полученных преступным путём, и финансирования терроризма, а также бухгалтерским, аудиторским, регуляторным требованиям.

При этом, Контролёром должно быть получено разрешение Комиссара, позволяющего Контролёру обрабатывать Персональные данные ограниченного доступа, применяя соответствующие защитные меры в отношении такой обработки. Разрешение получается на платной основе в порядке, предусмотренном Положением.

Большинство требований, касающихся безопасности обработки Персональных данных, схожи в обоих актах. Однако в отличие от GDPR, Положением прямо не предусмотрена возможность псевдонимизации или шифрования данных.

Согласно Положению, субъекты данных обладают большинством прав, предусмотренных GDPR, в том числе правом на информирование в отношении сбора и использования их данных; на доступ к данным; на удаление их данных (право на забвение); на исправление неточностей; на возражение против обработки; на подачу жалобы в адрес Комиссара. Однако некоторые права субъектов данных, указанные в GDPR, не предусмотрены Положением, в том числе право на переносимость данных, право на возражение против профилирования (Profiling) и автоматизированного принятия решений.

В контексте GDPR под “профилированием” понимается любая форма автоматизированной обработки персональных данных, состоящая из их использования для оценки определенных личных аспектов, касающихся физического лица, в частности для анализа или прогнозирования аспектов, касающихся производительности физического лица на работе, экономического положения, здоровья, его/её личных предпочтений, интересов, поведения, местоположения или перемещения (статья 4(4) GDPR).

С учётом стремительного развития информационных технологий, искусственного интеллекта, массового сбора и обработки данных через Интернет и социальные сети в настоящее время достаточно остро стоит проблема профилирования и автоматизированного принятия решений на основе полученных персональных данных. В западных странах было много громких судебных разбирательств по данному вопросу, по итогам которых в адрес некоторых крупных корпораций были начислены многомиллионные штрафы.

В Приложении № 3 к Правилам защиты данных МФЦА определены максимальные суммы штрафов, которые могут быть применены за нарушение Положения. Так, в случае предоставления недостоверной или вводящей в заблуждение информации Лицо может быть оштрафовано на сумму в размере 5 000 долларов США. В случае обработки Персональных данных ограниченного доступа в нарушение условий или запрета, предусмотренных в разрешении, размер штрафа составит 10 000 долларов США.

В случае передачи Персональных данных на территорию юрисдикции, не обеспечивающей достаточный уровень их защиты, Лицо может быть оштрафовано на 20 000 долларов США. Максимальный штраф в размере 25 000 долларов США предусмотрен за неисполнение указания по соблюдению законодательства МФЦА о защите Персональных данных.

## 5. Дополнительные комментарии

6.

Полагаем, что акты МФЦА в сфере защиты данных будут дополняться и совершенствоваться в процессе развития МФЦА. Действующее право МФЦА основывается на Конституции РК и состоит из: (i) Конституционного закона о МФЦА<sup>[6]</sup>; (ii) не противоречащих Конституционному закону о МФЦА актов Центра, которые могут быть основаны на принципах, нормах и прецедентах права Англии и Уэльса и (или) стандартах ведущих мировых финансовых центров, принимаемых органами МФЦА в пределах полномочий, предоставленных Конституционным законом о МФЦА; (iii) действующего права РК, которое применяется в части, не урегулированной Конституционным законом о МФЦА и актами МФЦА.

В связи с этим компаниям, зарегистрированным в МФЦА, необходимо иметь в виду, что Закон РК о защите персональных данных и иные подзаконные акты РК в сфере защиты персональных данных теоретически могут быть применены к их деятельности в части, не урегулированной Положением и Правилами о защите данных МФЦА. Полагаем, что в этом случае необходимо будет ориентироваться на будущую судебную практику Суда МФЦА (AIFC Court). Анализ судебных решений, размещенных в открытом доступе на сайте Суда МФЦА, показал отсутствие судебных кейсов, связанных с нарушением актов МФЦА в сфере защиты персональных данных<sup>[7]</sup>.

При этом стоит отметить, что в спорах, в которых стороны выбрали право МФЦА в качестве применимого права, при вынесении решений судьи опирались на акты, судебные решения МФЦА, нормы английского права и иногда делали ссылки на решения английских судов. Так, например, среди изученных судебных решений представлены дела, связанные с трудовыми спорами, по трудовым договорам, регулируемым Положением МФЦА о трудовых отношениях<sup>[8]</sup>. В этих судебных решениях судьи не применяли нормы Трудового кодекса РК. По нашим наблюдениям, судьи Суда МФЦА применяли казахстанское законодательство только при рассмотрении дел, по которым стороны выбрали право РК в качестве применимого права.

Даже если допустить теоретическую возможность применения Закона РК о персональных данных, это будет сложно сделать на практике, потому что большинство ключевых понятий Положения отсутствует в Законе РК о персональных данных. Например, нельзя провести аналогию между Контролёром и собственником базы, содержащей персональные данные, поскольку у этих лиц совершенно разный круг обязанностей.

Анализ казахстанской судебной практики также показывает, что судебных решений, касающихся правонарушений в сфере защиты персональных данных, очень мало. При этом большая часть дел, которые имеются в открытом доступе, были связаны, в первую очередь, с защитой чести, достоинства, деловой репутации, и в дополнение истцы ссылались на нарушение требований о защите персональных данных.

Как было отмечено ранее, судьи Суда МФЦА склонны ссылаться на решения английских судов, у которых в отличие от казахстанских судов имеется большой опыт разрешения споров в сфере защиты персональных данных. Положения GDPR были инкорпорированы в право Англии и Уэльса до выхода Великобритании из ЕС и наиболее известны как UK GDPR. Правовое регулирование защиты данных в Великобритании очень схоже с регулированием в ЕС. В связи с этим есть основания предполагать, что судьи МФЦА при разрешении споров в сфере защиты персональных данных будут скорее опираться на право МФЦА и английское право, чем на казахстанское законодательство.

За последние годы было много случаев нарушения требований о защите персональных данных, которые широко обсуждались в казахстанских СМИ. Мы рекомендуем компаниям, зарегистрированным в МФЦА, очень тщательно и осмотрительно относиться к вопросу защиты персональных данных для снижения риска нарушений и привлечения к ответственности.

---

[1] Публичный реестр МФЦА <https://publicreg.myafsa.com/roc/>.

[2] Положение МФЦА № 10 от 20 декабря 2017 года “О защите данных”.

[3] Правила МФЦА № 1 от 22 января 2018 года “О защите данных”.

[4] Регламент (ЕС) № 2016/679 от 27 апреля 2016 года Европейского парламента и Совета “О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы № 95/46/ЕС” (Общий регламент о защите персональных данных), наиболее часто используется аббревиатура **GDPR**.

[5] Закон РК от 21 мая 2013 года № 94-V “О персональных данных и их защите”.

[6] Конституционный закон РК от 7 декабря 2015 года № 438-V “О Международном финансовом центре «Астана”.

[7] По состоянию на 16 января 2024 года на сайте Суда МФЦА размещено 98 судебных дел за 2019-2023 годы.

[8] Положение № 4 МФЦА о трудовых отношениях от 20 декабря 2017 года.