Узбекистан | Декабрь 2022

УСИЛЕНИЕ ТРЕБОВАНИЙ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

05.10.2022 г. принято Постановление Кабинета Министров Республики Узбекистан (далее – «**РУз**») «Об утверждении некоторых нормативно-правовых актов в области обработки персональных данных» (далее – «**Постановление**») №570, которое вступает в силу с 07.01.2023 г. Ниже приводим основные, на наш взгляд, изменения, предусмотренные Постановлением.

Постановлением вводятся следующие Положения:

- об определении уровня защищенности персональных данных (далее – «**ПД**») при их обработке (далее – «**Положение №1**»);
- о требованиях к материальным носителям биометрических и генетических данных и технологиям хранения таких данных вне баз ПД (далее – «**Положение №2**»).

Положение №1

Определяются угрозы безопасности ПД при их обработке собственником и (или) оператором базы ПД, уровни защищенности и необходимые меры для обеспечения защиты ПД. Так угрозы безопасности ПД – это совокупность условий и факторов, которые могут повлечь изменение, дополнение, использование, предоставление, передачу, распространение, обезличивание, уничтожение, копирование ПД в результате несанкционированного, в том числе случайного доступа к базе ПД.

В зависимости от наличия недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении (далее – «**ПО**») баз ПД угрозы классифицируются на три типа:

i. Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном ПО баз ПД;
ii. Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном ПО баз ПД;
iii. Угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО баз ПД.

+7 705 209 91 59 | +998 97 727 0345
info@vakhidovlaw.com
vakhidovlaw.com

Вместе с тем, Постановлением определяются 4 уровня защиты ПД при обработке в базах ПД, которые должны обеспечиваться собственником и (или) оператором баз ПД. Определение уровня защиты, который должен обеспечиваться, производится в зависимости от наличия условий. К примеру, для установления **первого уровня** защиты ПД необходимо наличие минимум одного из следующих условий:

- наличие угроз 1-го типа и обработка специальных ПД[1] и (или) биометрических и (или) генетических данных;
- наличие угроз 2-го типа и обработка специальных ПД более 50 тыс. субъектов, не являющихся сотрудниками собственника и (или) оператора базы ПД.

Для установления **второго уровня** защиты необходимо наличие минимум одного из следующих условий:

- наличие угроз 1-го типа и обработка общедоступной информации;
- наличие угроз 2-го типа и обработка специальных ПД сотрудников или специальных ПД менее 50 тыс. субъектов, не являющихся сотрудниками собственника и (или) оператора;
- наличие угроз 2-го типа и обработка биометрических и (или) генетических данных;
- наличие угроз 2-го типа и обработка общедоступной информации более 50 тыс. субъектов, не являющихся сотрудниками собственника и (или) оператора;
- наличие угроз 3-го типа и обработка специальных ПД более 50 тыс. субъектов, не являющихся сотрудниками собственника и (или) оператора.

Для установления **третьего уровня** защиты необходимо наличие минимум одного из следующих условий:

- наличие угроз 2-го типа и обработка общедоступной информации: (i) сотрудников собственника и (или) оператора, (ii) менее 50 тыс. субъектов, не являющихся сотрудниками собственника и (или) оператора;
- наличие угроз 3-го типа и обработка специальных ПД: (i) сотрудников собственника и (или) оператора, (ii) менее 50 тыс. субъектов, не являющихся сотрудниками собственника и (или) оператора;
- наличие угроз 3-го типа и обработка биометрических и (или) генетических данных.

[1] Специальными персональными данными являются данные о расовом или социальном происхождении, политических, религиозных или мировоззренческих убеждениях, членстве в политических партиях и профессиональных союзах, а также данные, касающиеся физического или душевного (психического) здоровья, сведения о частной жизни и судимости (ст. 25 Закона РУз «О персональных данных» № ЗРУ-547 от 02 июля 2019 г.).

Для установления **четвертого уровня** защиты необходимо наличие угроз 3-го типа и обработка общедоступной информации.

Положение №2

Определяются требования к технологиям хранения биометрических и генетических данных вне баз ПД, а также требования к материальным носителям таких данных.

Среди основных требований можем отметить требование об обязательном наличии информации с грифом «Секретно» либо «Для служебного пользования» на материальных носителях, используемых для обработки биометрических и генетических данных.

Хранение биометрических и генетических данных в электронной форме допускается только в зашифрованном виде с использованием криптографического либо иного способа защиты. Также при хранении биометрических и генетических данных вне баз ПД необходимо соблюдать следующие требования:

- предоставление уполномоченным лицам собственника и (или) оператора базы биометрических и генетических данных доступа к ПД, хранящимся на материальном носителе;
- использование средств электронной цифровой подписи (ЭЦП) или иных информационных технологий, позволяющих сохранять целостность и неизменность биометрических и генетических данных, записанных на материальном носителе;
- проверка наличия письменного согласия субъекта на обработку биометрических и генетических данных или иных оснований для их обработки, предусмотренных законодательством.

Контакты:

Зафар Вахидов — Партнер, Vakhidov & Partners
Узбекистан / Казахстан
ZV@vakhidovlaw.com

Фатхулла Нигманов — Юрист, Vakhidov & Partners
Узбекистан
FatkhullaN@vakhidovlaw.com