УТВЕРЖДАЮ:
Председатель правления
ЖК "Киевская 147"

_____ А.М. Тайдонов
"____"_____20___г.

ПРАВИЛА

оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

Томск, 2018

1. Общие положения

1.1 Настоящие Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных (далее - Правила) определяют порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных", и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ №152-ФЗ.

1.2 Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

2. Основные понятия

2.1 В настоящих Правилах используются основные понятия:
2.1.1 Информация - сведения (сообщения, данные) независимо от формы их представления;
2.1.2 Безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;
2.1.3 Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
2.1.4 Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение;
2.1.5 Доступность информации - состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;
2.1.6 Убытки - расходы, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;
2.1.7 Моральный вред - физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом;
2.1.8 Оценка возможного вреда - определение уровня вреда на основании учета причиненных убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

3. Методика оценки возможного вреда субъектам персональных данных

3.1 Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2 Перечисленные неправомерные действия определяются как следующие нарушения:
3.2.1 Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;

3.2.2 Неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;
3.2.3 Неправомерное изменение персональных данных является нарушением целостности персональных данных;
3.2.4 Нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации;
3.2.5 Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;
3.2.6 Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объеме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных;
3.2.7 Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;
3.2.8 Принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или непредусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

3.3 Субъекту персональных данных может быть причинен вред в форме:
3.3.1 Убытков - расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;
3.3.2 Морального вреда - физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

3.4 В оценке возможного вреда ЖК "Киевская 147" исходит из следующего способа учета последствий допущенного нарушения принципов обработки персональных данных:
3.4.1 Низкий уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;
3.4.2 Средний уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных;
3.4.3 Высокий уровень возможного вреда - во всех остальных случаях.

4. Порядок проведения оценки возможного вреда, а также соотнесения возможного вреда и реализуемых ЖК "Киевская 147" мер

4.1 Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным в ЖК "Киевская 147" за защиту информации, в соответствии с методикой, описанной в разделе 3 настоящих Правил, и на основании экспертных значений, приведенных в Приложении №1.

4.2 Состав реализуемых ЖК "Киевская 147" мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ № 152-ФЗ "О персональных данных", определяется лицом, ответственным в ЖК "Киевская 147" за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.

Приложение 1

Оценка вреда, который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых ЖК "Киевская 147" мер

№ п\п	Требования Федерального закона "О персональных данных", которые могут быть нарушены	Возможные нарушение безопасности информации и причиненный субъекту вред		Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей оператора персональных данных
1.	Актуальность перечня должностных лиц, имеющих право самостоятельного доступа в помещения, где обрабатываются или хранятся персональные данные	Убытки и моральный вред		средний	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
		Целостность			
		Доступность	+		
		Конфиденциальность	+		
2.	Порядок доступа в помещения, где расположены элементы информационных систем персональных данных	Убытки и моральный вред		высокий	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		
3.	Порядок доступа в помещения, где обрабатываются и хранятся бумажные носители с персональными данными	Убытки и моральный вред		высокий	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		
4.	Наличие дополнительных запирающих устройств на местах хранения	Убытки и моральный вред		высокий	В соответствии с законодательством в области защиты информации и
		Целостность	+		

	документов с персональными данными	Доступность	+		Положением по обеспечению безопасности персональных данных
		Конфиденциальность	+		
5.	Состояние учета машинных носителей	Убытки и моральный вред		средний	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
		Целостность			
		Доступность	+		
		Конфиденциальность	+		
6.	Наличие учтенных съемных носителей персональных данных	Убытки и моральный вред	+	высокий	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
		Целостность			
		Доступность	+		
		Конфиденциальность	+		
7.	Наличие документов, содержащих персональные данные, без присмотра в открытом доступе в помещениях организации	Убытки и моральный вред	+	высокий	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		
8.	Своевременность исполнения запросов субъектов персональных данных	Убытки и моральный вред		низкий	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
		Целостность			
		Доступность	+		
		Конфиденциальность			
9.	Наличие необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в организации	Убытки и моральный вред	+	высокий	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
		Целостность			
		Доступность			
		Конфиденциальность	+		
10.	Актуальность информации о	Убытки и моральный вред		средний	В соответствии с законодательством

	законности целей обработки персональных данных	Целостность			в области защиты информации и Положением по обеспечению безопасности персональных данных
		Доступность			
		Конфиденциальность	+		
11.	Соответствие процедуры обработки персональных данных локальным документам и действующему законодательству Российской Федерации в области персональных данных	Убытки и моральный вред	+	высокий	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		
12.	Проверка сроков действия паролей	Убытки и моральный вред		высокий	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		
13.	Актуальность локальных нормативных актов по вопросам обработки и защиты персональных данных	Убытки и моральный вред		средний	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
		Целостность			
		Доступность			
		Конфиденциальность	+		
14.	Актуальность сведений, содержащихся в уведомлении Роскомнадзора об обработке (о намерении осуществлять обработку) персональных данных	Убытки и моральный вред		средний	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
		Целостность			
		Доступность			
		Конфиденциальность	+		
15.	Ознакомление работников с локальными нормативными актами, регламентирующими обработку	Убытки и моральный вред		средний	В соответствии с законодательством в области защиты информации и Положением по обеспечению
		Целостность			
		Доступность			

	персональных данных	Конфиденциальность	+		безопасности персональных данных
	наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;	Убытки и моральный вред	+	средний	Мониторинг средств защиты информации на наличие фактов доступа к ПД
		Целостность			
		Доступность			
		Конфиденциальность	+		
	мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;	Убытки и моральный вред		низкий	Применение резервного копирования
		Целостность	+		
		Доступность	+		
		Конфиденциальность			
	Контроль выполнения антивирусной политики	Убытки и моральный вред		низкий	
		Целостность	+		
		Доступность	+		
		Конфиденциальность			