Приложение № 6 к приказу
от «07» 02.2020 № 104

Правила
оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в МП «Калининградтеплосеть»

1. Общие положения

1.1. Настоящие Правила оценки возможного вреда субъектам персональных данных и принятия мер по его предотвращению (далее – Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных в случае нарушения Федерального закона № 152-ФЗ «О персональных данных» (далее - № 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных № 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 учёта причинённых 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 безопасности информации:

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 объёме 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 исключительно автоматизированной 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 причинён 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 МП «Калининградтеплосеть» исходит из следующего способа учёта 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 Оператором мер

4.1. Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным в МП «Калининградтеплосеть» за организацию обработки персональных данных, в соответствии с методикой, описанной в разделе 3 настоящих Правил, и на основании экспертных значений, приведённых в Приложении № 1.

4.2. Состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», определяется лицом, ответственным в МП «Калининградтеплосеть» за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.

Приложение к правилам оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в МП «Калининградтеплосеть»

ОЦЕНКА ВРЕДА, КОТОРЫЙ МОЖЕТ БЫТЬ ПРИЧИНЕН СУБЪЕКТАМ ПЕРСОНАЛЬНЫХ ДАННЫХ, А ТАКЖЕ СООТНЕСЕНИЕ ВОЗМОЖНОГО ВРЕДА И РЕАЛИЗУЕМЫХ В МП «КАЛИНИНГРАДТЕПЛОСЕТЬ» МЕР

№ п\п	Требования Федерального закона «О персональных данных», которые могут быть нарушены	Возможные нарушение безопасности информации		Причинённый субъекту вред (убытки и моральный вред)	Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей МП «Калининградтеплосеть», как оператора персональных данных
1.	Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей (часть 2 статьи 5)	Целостность		+	Высокий	Цели обработки персональных данных закреплены в «Перечень должностей, допущенных к обработке персональных данных с указанием используемых информационных систем». Внутренний контроль осуществляется в соответствии с «Правила осуществления внутреннего контроля».
		Доступность				
		Конфиденциальность	+			
2.	Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой (часть 3 статьи 5)	Целостность		+	Высокий	Соответствующие нормы закреплены в «Положение об обработке персональных данных» (п. 4.5). Внутренний контроль осуществляется в соответствии с «Правила осуществления внутреннего контроля».
		Доступность				
		Конфиденциальность	+			
3.	Обработке подлежат только персональные данные, которые отвечают целям их обработки (часть 4 статьи 5)	Целостность		+	Высокий	Категории субъектов персональных данных, ПДн которых обрабатываются в Обществе закреплены в «Перечень должностей, допущенных к обработке персональных данных с указанием используемых информационных систем». Внутренний контроль осуществляется в соответствии с «Правила осуществления внутреннего контроля».
		Доступность				
		Конфиденциальность	+			
4.	Содержание и объем обрабаты-	Целостность		+	Высокий	Соответствующие нормы закреплены в «Положе-

	ваемых персональных данных должны соответствовать заявленным целям обработки (часть 5 статьи 5)	Доступность				ние об обработке персональных данных» (п. 4.2). Внутренний контроль осуществляется в соответствии с «Правила осуществления внутреннего контроля»
		Конфиденциальность	+			
5.	При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных (часть 6 статьи 5)	Целостность	+	–	Низкий	Соответствующие нормы закреплены в «Положение об обработке персональных данных» (п. 4.4). Внутренний контроль осуществляется в соответствии с «Правила осуществления внутреннего контроля».
		Доступность				
		Конфиденциальность				
6.	Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных (часть 7 статьи 5)	Целостность		+	Высокий	Соответствующие нормы закреплены в «Положение об обработке персональных данных» (п. 6.3.2). Внутренний контроль осуществляется в соответствии с «Правила осуществления внутреннего контроля».
		Доступность				
		Конфиденциальность	+			
7.	Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом (статья 7)	Целостность		+	Высокий	Соответствующие нормы закреплены в «Положение об обработке персональных данных» (п. 3.2.2, 6.2.2). Внутренний контроль осуществляется в соответствии с «Правила осуществления внутреннего контроля».
		Доступность				
		Конфиденциальность	+			
8.	В целях информационного	Целостность		+	Высокий	Соответствующие нормы закреплены в «Положе-

	обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных (часть 1 статьи 8)	Доступность				ние об обработке персональных данных» (п. 6.4). Внутренний контроль осуществляется в соответствии с «Правила осуществления внутреннего контроля».
		Конфиденциальность	+			
9.	Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом (часть 1 статьи 9)	Целостность		+	Высокий	Согласия субъектов на обработку их персональных данных фиксируются надлежащим образом, позволяющим подтвердить факт их получения. Соответствующие нормы закреплены в «Положение об обработке персональных данных» (п. 5.1). Внутренний контроль осуществляется в соответствии с «Правила осуществления внутреннего контроля».
		Доступность				
		Конфиденциальность	+			
10.	Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, не-	Целостность	+	+	Средний	Соответствующие нормы закреплены в «Положение об обработке персональных данных» (п. 7.15). Запросы субъектов персональных данных фиксируются в системе электронного документооборота «Дело» Внутренний контроль осуществляется в соответствии с «Правила осуществления внутреннего
		Доступность				
		Конфиденциальность				

	точными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав (часть 1 статьи 14)					контроля».
11.	Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (часть 7 статьи 14)	Целостность		+	Средний	Соответствующие нормы закреплены в «Положение об обработке персональных данных» (п. 7.1.2). Запросы субъектов персональных данных фиксируются в системе электронного документооборота «Дело» Внутренний контроль осуществляется в соответствии с «Правила осуществления внутреннего контроля».
		Доступность	+			
		Конфиденциальность				