



ДУМА
УССУРИЙСКОГО ГОРОДСКОГО ОКРУГА

ПОСТАНОВЛЕНИЕ

22.02.2022

г. Уссурийск

№ 1

**Об утверждении Положения по обеспечению
безопасности персональных данных в Думе
Уссурийского городского округа**

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», Постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и в целях совершенствования работы по обеспечению защиты персональных данных в Думе Уссурийского городского округа (далее – Дума)

ПОСТАНОВЛЯЮ:

1. Утвердить Положение по обеспечению безопасности персональных данных (далее – ПДн) в Думе (прилагается).
2. Контроль по исполнению настоящего постановления возложить на заместителя председателя Думы.

Председатель Думы
Уссурийского городского округа

А.Н. Черныш

УТВЕРЖДЕНА

постановлением Думы
Уссурийского городского округа

от 22.02. 2022 года № 1

Положение по обеспечению безопасности
персональных данных в Думе Уссурийского
городского округа

1. Общие положения

1.1 Настоящее Положение определяет:

а) правовое основание обработки персональных данных (далее – ПДн) в Думе;

б) принципы обработки ПДн в Думе;

в) оценку вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон);

г) основные условия проведения обработки ПДн;

д) правила рассмотрения запросов субъектов ПДн или их представителей;

е) правила обработки и защиты ПДн;

ж) правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным Федеральным законом.

з) соотношение вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона, и мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом.

1.2. В настоящем Положении используются термины и определения в соответствии с Федеральным законом.

1.3. Субъектами ПДн в Думе являются:

а) работники Думы, а также лица, претендующие на замещение вакантных должностей в Думе;

б) физическое лицо, обращающееся в Думу по вопросам, входящим в ее компетенцию.

1.4. Объектами системы безопасности ПДн в Думе являются:

а) информационные ресурсы с ограниченным доступом, содержащие ПДн;

б) процессы обработки ПДн в информационных системах персональных данных (далее – ИСПДн) Думы, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал

разработчиков и пользователей системы и ее обслуживающий персонал;

в) информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки ПДн.

1.5. Дума, в пределах своих полномочий, имеет право создавать информационные системы (в том числе ИСПДн), информационные ресурсы необходимые для обеспечения ее деятельности.

1.6. Для каждой создаваемой информационной системы определяется цели обработки ПДн, перечень обрабатываемых ПДн.

2. Цели обработки ПДн в Думе

2.1 Обработка ПДн в Думе осуществляется в целях реализации трудовых отношений, а также в связи с необходимостью решения вопросов, входящих в ее компетенцию Думы.

2.2. Цели обработки ПДн в Думе соответствуют законодательству Российской Федерации, действующему в сфере обеспечения безопасности ПДн.

2.3. Цели обработки ПДн определяют:

- а) содержание и объем обрабатываемых ПДн;
- б) категории субъектов, ПДн которых обрабатываются;
- в) сроки их обработки и хранения.

3. Принципы обработки ПДн в Думе

3.1. Обработка ПДн в Думе осуществляется на основе следующих принципов:

а) обработка ПДн осуществляется в соответствии с действующим законодательством Российской Федерации;

б) обработка ПДн прекращается при достижении конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несоответствующая целям их сбора;

в) не допускается объединение баз ПДн, обработка которых осуществляется в разных целях;

г) обработке подлежат только ПДн, которые необходимы для достижения конкретных, законных целей;

д) содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки;

е) при обработке должны быть обеспечены их точность и актуальность, достаточные для достижения целей их обработки;

ж) оператор обеспечивает удаление (уточнение) неполных или неточных ПДн;

з) хранение ПДн должно осуществляться в форме, позволяющей

определить субъект ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен Федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обработываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

4. Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения правил обработки и защиты ПДн

4.1. Оценкой вреда, который может быть причинен субъектам ПДн в случае нарушения правил обработки и защиты ПДн.

4.2. Под юридическими последствиями в настоящем Положении понимаются случаи возникновения или прекращения личных либо имущественных прав граждан, или иные обстоятельства каким-либо образом затрагивающие их его права, свободы и законные интересы.

4.3. При обработке ПДн должны определяться и документально оформляться все последствия, затрагивающие права и законные интересы субъекта ПДн, которые могут возникнуть в случае нарушения правил обработки и защиты ПДн.

4.4. Определение юридически значимых последствий необходимо для недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты его прав на неприкосновенность частной жизни, личную и семейную тайну, а также для определения соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер.

5. Перечень действий (операций) совершаемых с ПДн в Думе

5.1. В Думе применяются следующие способы получения ПДн субъектов ПДн:

- а) заполнение субъектом ПДн соответствующих форм;
- б) получение ПДн от третьих лиц;
- в) получение ПДн на основании запроса по форме согласно Приложению 6 к Положению;
- г) сбор ПДн из общедоступных источников.

5.2. Если в соответствии с действующим законодательством Российской Федерации, предоставление ПДн является обязательным. Дума обязана разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн по форме согласно Приложению 3 к Положению.

5.3. Если ПДн получены не от субъекта ПДн, до начала обработки таких ПДн обязана предоставить субъекту ПДн уведомление об обработке ПДн по

форме согласно Приложению 9 к Положению.

5.4. При сборе ПДн обеспечивается запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона.

5.5. Систематизация, накопление, уточнение и использование ПДн.

5.6. Систематизация, накопление, уточнение, использование ПДн могут осуществляться любыми законными способами в соответствии с правилами, инструкциями, руководствами, регламентами и иными документами, определяющими технологический процесс обработки информации. В Думе могут быть установлены особенности учета ПДн в ИСПДн, в том числе использование различных способов обозначения принадлежности ПДн, содержащихся в соответствующей ИСПДн, конкретному субъекту ПДн.

5.7. Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки ПДн или обозначения принадлежности ПДн, содержащихся в ИСПДн, конкретному субъекту ПДн. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности ПДн, содержащихся в ИСПДн, конкретному субъекту ПДн.

5.8. Уточнение ПДн должно производиться только на основании законно полученной в установленном порядке информации. При необходимости, уведомление об уточнении ПДн осуществляется в письменном виде по форме согласно Приложению 8 к Положению.

5.9. Использование ПДн должно осуществляться исключительно в заявленных целях. Использование ПДн в заранее не определенных и не оформленных установленным образом целях категорически не допускается.

5.10. Запись и извлечение ПДн.

5.11. Запись ПДн в ИСПДн Думы может осуществляться с любых носителей информации или из других ИСПДн.

5.12. Извлечение ПДн из ИСПДн может осуществляться с целью:

а) вывода ПДн на бумажный или иной носитель информации, не предназначенный для его обработки средствами вычислительной техники;

б) вывода ПДн на носители информации, предназначенные для их обработки средствами вычислительной техники.

При извлечении ПДн должен проводиться учет носителей информации.

5.13. При осуществлении записи и (или) извлечения ПДн должны соблюдаться условия обработки ПДн, конфиденциальность ПДн и иные требования, указанные в Положении.

5.14. Передача ПДн.

5.15. Передача ПДн в Думе должна осуществляться с соблюдением Положения и действующего законодательства Российской Федерации.

5.16. В Думе приняты следующие способы передачи ПДн субъектов ПДн:

а) передача ПДн на электронных и бумажных носителях информации

нарочным способом;

б) передача ПДн на электронных и бумажных носителях посредством почтовой связи;

в) передача ПДн по каналам связи.

5.17. Перед осуществлением передачи ПДн проверяется основание на осуществление такой передачи и наличие согласия на передачу ПДн в согласии субъекта ПДн на обработку ПДн или наличие иных законных оснований.

5.18. Передача ПДн должна осуществляться на основании:

а) договора с третьей стороной, которой осуществляется передача ПДн;

б) запроса, полученного от третьей стороны, которой осуществляется передача ПДн;

В случае исполнения лицами Думы функций, полномочий и обязанностей, возложенных в соответствии с действующим законодательством Российской Федерации.

5.19. Передача ПДн без согласия работника или в отсутствии иных законных оснований категорически запрещается.

5.20. Хранение ПДн.

5.21. Хранение ПДн в Думе допускается только в форме документов – зафиксированной на материальном носителе информации (содержащей ПДн) с реквизитами, позволяющими ее идентифицировать и определить субъекта ПДн. При этом предусматриваются следующие виды документов:

а) изобразительный документ – документ, содержащий информацию, выраженную посредством изображения какого-либо объекта;

б) фотодокумент – изобразительный документ, созданный фотографическим способом;

в) текстовый документ – документ, содержащий речевую информацию, зафиксированную любым типом письма или любой системой звукозаписи;

г) письменный документ – текстовый документ, содержащий информацию, зафиксированную любым типом письма;

д) рукописный документ – письменный документ, при создании которого знаки письма нанесены от руки;

е) машинописный документ – письменный документ, при создании которого знаки письма нанесены техническими средствами;

ж) документ на машинном носителе – документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

Хранение ПДн в ИСПДн Думы и вне таких систем осуществляется только на таких материальных носителях информации и с применением такой технологии ее хранения, которая обеспечивает защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

Определение сроков хранения осуществляется в соответствии с требованиями законодательства Российской Федерации в сфере архивного

дела.

При использовании документов, содержащих ПДн, в различных целях определение сроков обработки, в том числе хранения, таких документов устанавливается по максимальному сроку.

Включение в состав Архивного фонда Российской Федерации документов, содержащих ПДн, осуществляется на основании экспертизы ценности документов.

Сроки временного хранения документов, включенных в состав Архивного фонда Российской Федерации, до их поступления в муниципальный архив, устанавливаются в соответствии с требованиями архивного законодательства Российской Федерации.

Документы Архивного фонда Российской Федерации, находящиеся в собственности Думы, по истечении сроков их временного хранения передаются на постоянное хранение в муниципальный архив.

5.22. Блокирование ПДн.

5.23. Блокированием ПДн называется временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Блокирование ПДн конкретного субъекта ПДн должно осуществляться во всех ИСПДн Думы, включая архивы баз данных, содержащих такие ПДн.

5.24. Блокирование ПДн в Думе осуществляется:

а) в случае выявления неправомерной обработки ПДн на основании обращения субъекта ПДн или его представителя, либо по запросу субъекта ПДн или его представителя по форме согласно Приложению 12 Положению, либо уполномоченного органа по защите прав субъектов ПДн с момента такого обращения или получения указанного запроса на период проверки ПДн;

б) в случае отсутствия возможности уничтожения ПДн в установленные сроки.

5.25. Обезличивание ПДн.

Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

Требования и методы по обезличиванию ПДн, обрабатываемых в информационных системах ПДн, установлены приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05 сентября 2013 года № 996.

Под обезличиванием ПДн понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Обезличивание ПДн должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки.

Работники отделов аппарата Думы, непосредственно осуществляющие обработку ПДн, готовят предложения по обезличиванию ПДн, обоснование такой необходимости и способ обезличивания, осуществляют обезличивание

выбранным способом.

5.26. Уничтожение ПДн.

Уничтожение ПДн – это действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Уничтожение ПДн в Думе производится только в следующих случаях:

а) ПДн являются незаконно полученными, или не являются необходимыми для заявленной цели обработки;

б) в случае выявления неправомерной обработки ПДн, если обеспечить правомерность обработки ПДн невозможно;

При уничтожении ПДн необходимо:

а) убедиться в необходимости уничтожения ПДн;

б) убедиться в том, что уничтожаются те ПДн, которые предназначены для уничтожения;

в) уничтожить ПДн подходящим способом, в соответствии с настоящим Положением или способом, указанным в соответствующем требовании или распорядительном документе;

г) проверить необходимость уведомления об уничтожении ПДн;

д) при необходимости, уведомить об уничтожении ПДн требуемых лиц в письменном виде по формам согласно Приложениям 4, 10 к настоящему Положению.

При уничтожении ПДн применяются следующие способы:

а) измельчение в бумагорезательной (бумагоуничтожительной) машине – для документов, исполненных на бумаге;

б) стирание ПДн – для сохранения возможности обработки иных данных, зафиксированных на материальном носителе, содержащем ПДн;

в) физическое уничтожение (разрушение) носителей информации – для носителей информации на оптических дисках;

г) физическое уничтожение частей носителей информации (разрушение или сильная деформация) – для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); SSD-дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);

д) стирание с помощью сертифицированных средств уничтожения информации – для записей в базах данных и отдельных документов на машинном носителе.

При уничтожении ПДн необходимо учитывать их наличие в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено действующим законодательством Российской Федерации.

При необходимости уничтожения части ПДн допускается уничтожать материальный носитель одним из указанных в настоящем Положении способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению.

Уничтожение ПДн производится только в присутствии лица, ответственного за организацию обработки ПДн в Думе.

По факту уничтожения ПДн составляется Акт уничтожения ПДн, который подписывается лицами, производившими уничтожение.

Хранение актов уничтожения ПДн осуществляется в течение срока исковой давности, если иное не установлено нормативными правовыми актами Российской Федерации.

6. Права субъектов ПДн

6.1. Круг субъектов, ПДн которых подлежат обработке в ИСПДн Думы определяется целью обработки ПДн в каждой информационной системе ПДн.

6.2. При обращении в соответствии с формами согласно Приложениям 13, 14, 16 к настоящему Положению субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей следующие сведения:

- а) правовые основания и цель обработки ПДн;
- б) способы обработки ПДн;
- в) сведения о лицах (за исключением работников Думы), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Думой или на основании федерального закона;
- г) источник их получения обрабатываемых ПДн;
- д) сроки хранения и обработки ПДн;
- е) порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом;
- ж) информацию об осуществленной или о предполагаемой трансграничной передаче данных.

6.3. Право субъекта ПДн на доступ к своим ПДн может быть ограничено в соответствии с Федеральным законом в случае, если:

- а) обработка ПДн, включая ПДн, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- б) обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- в) доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

6.4. Если субъект ПДн считает, что Дума осуществляет обработку его ПДн с нарушением требований Федерального закона или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Думы в уполномоченном органе по защите прав субъектов ПДн или в судебном порядке.

6.5. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию

морального вреда в судебном порядке.

6.6. Дума освобождается от обязанности предоставить субъекту ПДн сведения, предусмотренные пунктом 26, в случаях, если:

- а) субъект ПДн уведомлен об осуществлении обработки его ПДн Думой;
- б) ПДн получены Думой на основании Федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- в) ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
- г) Дума осуществляет обработку ПДн для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;
- д) предоставление субъекту ПДн сведений, нарушает права и законные интересы третьих лиц.

7. Основные условия проведения обработки ПДн

7.1. Обработка ПДн осуществляется после получения согласия субъекта ПДн, составленного по форме согласно приложению № 1 к настоящему Положению, за исключением случаев, предусмотренных Федеральным законом.

ПДн могут быть получены оператором от лица, не являющегося субъектом ПДн, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона.

7.2. Работник при обработке ПДн принимает все необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

7.3. В каждом отделе аппарата Думы назначается лицо, ответственное за обеспечение безопасности ПДн. Данные лица взаимодействуют по вопросам организации защиты ПДн в ИСПДн с отделом информационного обеспечения аппарата Думы.

7.4. Начальники отделов аппарата Думы, в чьем ведении находится ИСПДн, определяют лиц, допущенных к обработке ПДн, и представляют списки данных лиц в отдел информационного обеспечения аппарата Думы.

7.5. Лица, допущенные к обработке ПДн, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации, содержащей ПДн, по форме согласно приложению 2 к настоящему Положению.

7.6. Оператором и третьими лицами, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных. Оператор или иное

получившее доступ к ПДн лицо обязано не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

7.7. В случае если оператор на основании договора поручает обработку ПДн другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности ПДн и безопасности ПДн при их обработке.

8. Способы обработки ПДн в информационных системах ПДн в зависимости от применения средств автоматизации

Способы обработки ПДн в ИСПДн Думы:

- а) обработка ПДн с использованием средств автоматизации;
- б) обработка ПДн без использования средств автоматизации;
- в) исключительно автоматизированная обработка ПДн;
- г) смешанная обработка ПДн.

9. Правила обработки и защиты ПДн в информационных системах с использованием средств автоматизации

9.1. Обработка ПДн в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями, утвержденными Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

9.2. Оператор ИСПДн определяет тип угроз безопасности ПДн, актуальных для ИСПДн, с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона, и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона.

9.3. Под актуальными угрозами безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного доступа к ПДн при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия.

9.4. Угрозы 1-го типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении (далее – ПО), используемом в информационной системе.

9.5. Угрозы 2-го типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном ПО,

используемом в информационной системе.

9.6. Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО, используемом в информационной системе.

9.7. Оператор ИСПДн на основании типа угроз определяет уровень защищенности ПДн в зависимости от категории обрабатываемых данных и их количества.

При обработке ПДн в информационных системах устанавливаются 4 уровня защищенности ПДн.

9.8. Необходимость обеспечения 1-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории ПДн, либо биометрические ПДн, либо иные категории ПДн;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора.

9.9. Необходимость обеспечения 2-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные ПДн;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории ПДн работников оператора или специальные категории ПДн менее чем 100000 субъектов ПДн, не являющихся работниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические ПДн;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора.

9.10. Необходимость обеспечения 3-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные ПДн работников оператора или общедоступные ПДн менее чем 100000 субъектов ПДн, не

являющихся работниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории ПДн работников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся работниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории ПДн работников оператора или специальные категории ПДн менее чем 100000 субъектов ПДн, не являющихся работниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические ПДн;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора.

9.11. Необходимость обеспечения 4-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные ПДн;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории ПДн работников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся работниками оператора.

9.12. Для обеспечения 4-го уровня защищенности ПДн при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей ПДн;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации (далее – СЗИ), прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

9.13. Не допускается обработка ПДн в ИСПДн с использованием средств автоматизации при отсутствии:

а) утвержденных организационно-технических документов о порядке эксплуатации информационных систем ПДн, включающих акт классификации ИСПДн, инструкции пользователя, администратора по организации антивирусной защиты, парольной защиты автоматизированных систем, и

других нормативных и методических документов;

б) настроенных СЗИ от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;

в) охраны и организации режима допуска в помещения, предназначенные для обработки ПДн.

10. Правила обработки и защиты ПДн в информационных системах без использования средств автоматизации

10.1. Обработка ПДн без использования средств автоматизации (в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации) осуществляется в соответствии с Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации».

10.2. Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн были:

а) определены места хранения ПДн (материальных носителей) и установлен перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ;

б) обеспечено раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях;

в) соблюдены условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

10.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;

б) типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, - при необходимости получения письменного согласия на обработку ПДн;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав

и законных интересов иных субъектов ПДн;

г) типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

10.4. При использовании внешних электронных носителей информации с ПДн данные электронные носители информации, учитываются в журнале учета, выдачи и уничтожения машинных носителей данных, предназначенных для обработки и хранения информации ограниченного доступа, не относящейся к государственной тайне, ПДн в Думе.

10.5. Все документы, содержащие ПДн, должны храниться в служебных помещениях в недоступных для посторонних лиц местах, надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы условия, обеспечивающие их сохранность.

11. Правила исключительно автоматизированной обработки ПДн

11.1. При исключительно автоматизированной обработке ПДн должны выполняться правила обработки ПДн средствами автоматизации, указанные в разделе 10 настоящего Положения.

11.2. Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПДн только при наличии согласия в письменной форме субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.

11.3. В остальных случаях принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, запрещается.

11.4. При исключительно автоматизированной обработке ПДн необходимо:

- а) разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его ПДн;
- б) разъяснить возможные юридические последствия такого решения;
- в) предоставить возможность заявить возражение против такого решения;
- г) рассмотреть возражение;
- д) уведомить субъекта ПДн о результатах рассмотрения такого возражения в течение тридцати дней со дня получения возражения.

12. Правила смешанной обработки ПДн

При смешанной обработке ПДн необходимо выполнять правила объединяющие правила обработки ПДн с использованием средств

автоматизации, указанные в разделе 10 настоящего Положения, и правила обработки ПДн без использования средств автоматизации, указанные в разделе 11 настоящего Положения.

13. Правила обработки ПДн средствами автоматизации при поручении обработки ПДн третьему лицу

13.1. Дума вправе поручить обработку ПДн третьему лицу (далее – поручение оператора):

а) с согласия субъекта ПДн и если иное не предусмотрено Федеральным законом;

б) на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта.

Лицо, осуществляющее обработку ПДн по поручению оператора, обязано соблюдать принципы и правила обработки ПДн, предусмотренные настоящим Положением.

13.2. В поручении оператора:

а) должен быть определен перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн;

б) должны быть определены цели обработки ПДн;

в) должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн;

г) должна быть установлена обязанность такого лица обеспечивать безопасность ПДн при их обработке;

д) должны быть указаны требования к защите обрабатываемых ПДн в соответствии с настоящим Положением и техническим заданием на создание системы защиты ПДн;

е) установлена ответственность такого лица перед Думой, в случаях нарушений установленных требований и законодательства Российской Федерации в области ПДн;

ж) при необходимости получения согласий на обработку ПДн от субъектов ПДн предусмотрен порядок сбора и передачи в Думу таких согласий субъектов ПДн.

13.3. В случае если Дума поручает обработку ПДн третьему лицу, ответственность перед субъектом ПДн за действия указанного лица несет Дума.

13.4. В случае необходимости получения согласия на обработку ПДн от субъекта ПДн, обязанность получения таких согласий возлагается на Думу.

14. Правила обработки обезличенных ПДн

14.1. Обезличенные ПДн не подлежат разглашению и нарушению конфиденциальности.

14.2. Обезличенные ПДн могут обрабатываться с использования и без

использования средств автоматизации.

14.3. При обработке обезличенных ПДн с использованием средств автоматизации необходимо соблюдение:

- а) инструкции по паролям;
- б) инструкции по антивирусу;
- г) инструкции по резервному копированию.

15. Правила обработки специальных категорий ПДн

15.1. Обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, если:

- а) субъект ПДн дал согласие в письменной форме на обработку своих ПДн;
- б) ПДн сделаны общедоступными субъектом ПДн;
- в) обработка ПДн осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;
- г) обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан.

15.2. Обработка ПДн о судимости может осуществляться Думой в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации.

15.3. Обработка специальных категорий ПДн, осуществлявшаяся в случаях, предусмотренных пунктами 15.1 и 15.2 настоящего Положения.

16. Правила обработки общедоступных ПДн

16.1. Общедоступные ПДн физических лиц, полученные из сторонних общедоступных источников ПДн, в Думе обрабатываются в исключительных случаях в сроки, не превышающие необходимых для их использования. При этом совместно с такими данными должны собираться реквизиты их источника и подтверждение согласия субъекта ПДн на включение такой информации в общедоступные источники ПДн, так как в случае обработки общедоступных ПДн обязанность доказывания того, что обрабатываемые ПДн являются общедоступными, возлагается на Думу. По достижении целей обработки общедоступных ПДн они подлежат немедленному уничтожению.

16.2. В целях информационного обеспечения в Думе могут создаваться общедоступные источники ПДн (в том числе справочники, адресные книги). В общедоступные источники ПДн с письменного согласия субъекта ПДн, по форме согласно приложению 18 к Положению, могут включаться его фамилия, имя, отчество, дата рождения, служебный номер телефона, занимаемая

должность, сведения о профессии и иные ПДн, сообщаемые субъектом ПДн.

16.3. Сведения о субъекте ПДн должны быть в любое время исключены из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

17. Обеспечение безопасности ПДн в Думе

17.1. С целью защиты субъектов ПДн Думы от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на ПДн, их носители, процессы обработки и передачи в Думе создается система безопасности ПДн, включающая в себя организационные меры и средства защиты информации (далее – СЗИ), а также используемые в информационной системе информационные технологии.

17.2. Система безопасности ПДн Думе обеспечивает решение следующих задач:

а) своевременное выявление, оценку и прогнозирование источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба заинтересованным субъектам ПДн, нарушению нормального функционирования ИСПДн Думы;

б) создание механизма оперативного реагирования на угрозы безопасности ПДн;

в) создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн;

г) защиту от вмешательства в процесс функционирования ИСПДн Думы посторонних лиц;

д) разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Думы, то есть защиту от несанкционированного доступа;

е) обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

ж) защиту от несанкционированной модификации используемых в ИСПДн Думы программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

з) защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

17.3. В рамках реализации системы безопасности ПДн в Думе проводятся следующие мероприятия:

а) строгий учет всех подлежащих защите ресурсов ИСПДн Думы (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

- б) регистрация действий персонала, осуществляющего обслуживание и модификацию программных и технических средств ИСПДн;
- в) разработка организационно-распорядительных документов по вопросам обеспечения безопасности информации;
- г) подготовка лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности ПДн и процессов их обработки;
- д) наделение каждого работника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к ИСПДн Думы;
- е) соблюдение всеми пользователями ИСПДн Думы требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
- ж) несение персональной ответственности за свои действия (в рамках своих функциональных обязанностей) каждого работника, имеющего доступ к ИСПДн Думы;
- з) поддержание необходимого уровня защищенности элементов ИСПДн Думы;
- и) применение физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
- к) контроль за соблюдением пользователями ИСПДн Думы требований по обеспечению безопасности информации;
- л) защита интересов Думы при взаимодействии с внешними организациями (связанном с обменом ПДн) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

18. Контроль и надзор за соблюдением правил по обработке и защите ПДн

18.1. Контроль и надзор за соблюдением правил по обработке и защите ПДн в Думе состоит из следующих направлений:

- а) внешний контроль и надзор за соблюдением правил по обработке и защите ПДн;
- б) внутренний контроль и надзор за соблюдением правил по обработке и защите ПДн.

18.2. Внутренний контроль и надзор за соблюдением правил по обработке и защите ПДн в Думе состоит из:

- а) контроля и надзора за исполнением правил по обработке и защите ПДн;
- б) оценки соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер.

18.3. Внешний контроль и надзор за выполнением требований законодательства в области ПДн осуществляется федеральным органом

исполнительной власти, осуществляющим функции по контролю и надзору в сфере информационных технологий и связи, федеральным органом исполнительной власти; уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

18.4. Внешний контроль и надзор за выполнением требований законодательства в области ПДн осуществляется в соответствии с действующим законодательством Российской Федерации в области защиты прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля, подзаконных нормативных актов Правительства Российской Федерации, ведомственных нормативных актов и административных регламентов.

18.5. Уполномоченным органом по защите прав субъектов ПДн, на который возлагается обеспечение контроля и надзора за соответствием обработки ПДн требованиям Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

18.6. Уполномоченный орган по защите прав субъектов ПДн имеет право:

а) запрашивать у Думы информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

б) осуществлять проверку сведений, содержащихся в уведомлении об обработке ПДн Думы, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

в) требовать от Думы уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем ПДн;

г) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства в области ПДн;

д) обращаться в суд с исковыми заявлениями в защиту прав субъектов ПДн, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов ПДн в суде;

е) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, необходимые сведения;

ж) направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн, в соответствии с подведомственностью;

з) привлекать к административной ответственности лиц, виновных в нарушении Федерального закона.

18.7. В отношении ПДн, ставших известными уполномоченному органу

по защите прав субъектов ПДн в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность ПДн.

18.8. Решения уполномоченного органа по защите прав субъектов ПДн могут быть обжалованы в судебном порядке.

18.9. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности ПДн, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с ПДн, обрабатываемыми в ИСПДн.

19. Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн в Думе

19.1. В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям в Думе организуется проведение периодических проверок условий обработки ПДн.

Проверки осуществляются лицом, ответственным за организацию обработки ПДн в Думе, на основании утвержденного Плана внутренних проверок условий обработки ПДн в Думе.

19.2. При осуществлении внутреннего контроля соответствия обработки ПДн установленным требованиям в Думе производится проверка:

- а) соблюдения принципов обработки ПДн;
- б) соответствия нормативных правовых актов Думы в области ПДн действующему законодательству Российской Федерации;
- в) выполнения работниками Думы требований и правил обработки ПДн в ИСПДн Думы;
- г) актуальности информации о законности целей обработки ПДн и вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн;
- д) правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой ИСПДн Думе;
- е) актуальности перечня работников Думы, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн;
- ж) соблюдения обязанностей Думы, предусмотренных действующим законодательством в области ПДн;
- з) порядка взаимодействия с субъектами ПДн, чьи ПДн обрабатываются в ИСПДн Думы, в том числе соблюдения сроков, предусмотренных действующим законодательством в области ПДн, соблюдения требований об

уведомлениях, порядка доведения субъектам ПДн необходимой информации, порядка реагирования на обращения субъектов ПДн, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами ПДн;

к) наличия необходимых согласий субъектов ПДн, чьи ПДн обрабатываются в ИСПДн Думы;

л) актуальности сведений, содержащихся в уведомлении Думы об обработке ПДн;

м) актуальности перечня ИСПДн в Думы;

о) знаний и соблюдения работниками Думы положений действующего законодательства Российской Федерации, нормативных правовых актов Думы в области обработки и обеспечения безопасности ПДн;

п) знаний и соблюдения работниками Думы и инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе ПО, и СЗИ;

р) соблюдения работниками Думы конфиденциальности ПДн;

с) актуальности нормативных правовых актов Думы в области обеспечения безопасности ПДн;

т) соблюдения работниками Думы требований по обеспечению безопасности ПДн;

у) наличия нормативных правовых актов Думы, технической и эксплуатационной документации технических и программных средств ИСПДн Думы;

ф) иных вопросов.

19.3. По результатам проведенной проверки оформляется Акт внутренней проверки состояния защиты ПДн в Думе.

20. Оценка соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн

20.1. Во время осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям в Думе производится оценка соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения правил обработки и защиты ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн в Думе.

20.2. При оценке соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн, для каждой ИСПДн Думы производится экспертное сравнение заявленной Думой оценки вреда, который может быть причинен субъектам ПДн в случае нарушения правил обработки и защиты ПДн и применяемых Думой мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области

ПДн и изложенных в настоящем Положении.

20.3. По итогам сравнений принимается решение о достаточности применяемых Думой мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПДн, и возможности или необходимости принятия дополнительных мер или изменения установленного в Думе порядка обработки и обеспечения безопасности ПДн.

20.4. Оценка соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн в Думе оформляется в виде отдельного документа.

20.5. По результатам принятых решений лицом, ответственным за организацию обработки ПДн в Думе организуется работа по их реализации.

21. Ответственность лиц

21.1. Работники Думы, допущенные к ПДн, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

21.2. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, а также требований к защите ПДн подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков.

Приложение 1
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

СОГЛАСИЕ
на обработку персональных данных

Я, _____,
(Ф.И.О.) серия _____ N _____
(вид документа, удостоверяющего личность)
выдан _____
(когда и кем)
проживающий(ая) по адресу: _____
_____ в целях _____
(цель обработки персональных данных)
даю согласие _____
(наименование и адрес оператора)
на обработку моих персональных данных, а именно: _____
_____,
(перечень персональных данных)
то есть на осуществление любых действий (операций) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение персональных данных, в том числе на передачу, доступ, распространение, предоставление персональных данных определенному кругу лиц (в том числе, на обработку персональных данных по поручению оператора другому лицу):

(наименование и адрес лица, осуществляющего обработку персональных данных по поручению оператора)

(если обработка будет поручена такому лицу)

Настоящее согласие действует со дня его подписания и дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.
Настоящее согласие может быть отозвано в соответствии с законодательством Российской Федерации.

_____ (фамилия, инициалы лица, давшего согласие) _____ (подпись)
" ____ " _____ Г.

Приложение 2
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

ОБЯЗАТЕЛЬСТВО
О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Я, _____,
(Ф.И.О)

исполняющий(ая) должностные обязанности по замещаемой должности

(должность, наименование структурного подразделения)
предупрежден(а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному руководителю.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. После прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

(фамилия, инициалы)

(подпись)

" ____ " _____ Г.

Приложение 3
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

Разъяснение
субъекту персональных данных юридических последствий
отказа предоставить свои персональные данные

Уважаемый(ая) _____ !

В соответствии с требованиями Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" уведомляем Вас, что обязанность предоставления Вами персональных данных установлена _____

(реквизиты и наименование нормативных правовых актов)

В случае отказа Вами предоставить свои персональные данные, оператор не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям _____

(перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи иным образом затрагивающие его права, свободы и законные интересы)

В соответствии с законодательством в области персональных данных Вы имеете право:

на получение сведений об операторе, о месте его нахождения, о наличии у оператора своих персональных данных, а также на ознакомление с такими персональными данными;

требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

на получение при обращении или при направлении запроса информации, касающейся обработки своих персональных данных;

на обжалование действия или бездействия оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

(должность)

(подпись)

(Ф.И.О.)

" ____ " _____ 20__ г.

Приложение 4
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

(указать уполномоченный орган)

УВЕДОМЛЕНИЕ ОБ УНИЧТОЖЕНИИ

Настоящим уведомлением сообщаем Вам, что в связи с _____
персональные данные _____

(указать персональные данные)
уничтожены.

(должность)

(подпись)

(Ф.И.О.)

"__" _____ 20__ г.

Приложение 5
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

(указать уполномоченный орган)

УВЕДОМЛЕНИЕ
ОБ УСТРАНЕНИИ ДОПУЩЕННЫХ НАРУШЕНИЙ

Настоящим уведомлением сообщаем Вам, что допущенные нарушения при
обработке персональных данных, а именно _____

(указать допущенные нарушения)
устранены.

(должность)

(подпись)

(Ф.И.О.)

"__" _____ 20__ г.

Приложение 6
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

ЗАПРОС

Уважаемый(ая) : _____ (Ф.И.О.), в
связи с _____ у Думы Уссурийского городского
округа возникла необходимость получения следующей информации, составляющей
Ваши персональные данные _____

(перечислить информацию)

Просим Вас предоставить указанные сведения в течение _____ рабочих
дней с момента получения настоящего запроса.

В случае невозможности предоставить указанные сведения просим в
указанный срок дать письменное согласие на получение нами необходимой
информации из следующих источников _____,
следующими способами _____.

По результатам обработки указанной информации нами планируется принятие
следующих решений, которые будут доведены до Вашего сведения

Против принятого решения Вы имеете право заявить свои письменные
возражения в _____ срок.

(должность)

(подпись)

(Ф.И.О.)

" ____ " _____ 20__ г.

Приложение 7
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

УВЕДОМЛЕНИЕ О БЛОКИРОВАНИИ

Уважаемый(ая) _____ (Ф.И.О.),
в связи с _____ сообщаем Вам, что Ваши
персональные данные _____
(указать персональные данные)
заблокированы на срок _____.

(должность) (подпись) (Ф.И.О.)

"__" _____ 20__ г.

Приложение 8
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

УВЕДОМЛЕНИЕ ОБ УТОЧНЕНИИ

Уважаемый (ая) _____ (Ф.И.О.), в связи с
_____ сообщаем Вам, что Ваши персональные данные
уточнены в соответствии со сведениями:
_____.

(должность)

(подпись)

(Ф.И.О.)

"__" _____ 20__ г.

Приложение 9
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

УВЕДОМЛЕНИЕ

Уважаемый(ая) _____ (Ф.И.О.),
Думой Уссурийского городского округа производится обработка
сведений, составляющих Ваши персональные данные: _____

(указать сведения)

Цели обработки: _____.

Способы обработки: _____.

Перечень лиц, которые имеют доступ к информации, содержащей Ваши
персональные данные или могут получить такой доступ:

N	Должность	Ф.И.О.	Вид доступа	Примечания

По результатам обработки указанной информации нами планируется принятие
следующих решений, которые будут доведены до Вашего сведения

Против принятого решения Вы имеете право заявить свои письменные
возражения в _____ срок.

(должность)

(подпись)

(Ф.И.О.)

" ____ " _____ 20__ г.

Приложение 10
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

УВЕДОМЛЕНИЕ ОБ УНИЧТОЖЕНИИ

Уважаемый(ая) _____ (Ф.И.О.),
в связи с _____ сообщаем
Вам, что Ваши персональные данные _____

(указать персональные данные)
уничтожены.

(должность) (подпись) (Ф.И.О.)

" ____ " _____ 20__ г.

Приложение 11
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

УВЕДОМЛЕНИЕ
ОБ УСТРАНЕНИИ ДОПУЩЕННЫХ НАРУШЕНИЙ

Уважаемый(ая) _____ (Ф.И.О.), в связи с
_____ сообщаем Вам, что все допущенные нарушения
при обработке Ваших персональных данных устранены.

(должность)

(подпись)

(Ф.И.О.)

" ____ " _____ 20__ г.

Приложение 12
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

В _____
от _____
(Ф.И.О. заявителя)

(наименование и реквизиты
документа, удостоверяющего
личность заявителя)

ЗАЯВЛЕНИЕ

Прошу заблокировать обрабатываемые Вами мои персональные данные:

_____ (указать блокируемые персональные данные)
на срок: _____ ;
_____ (указать срок блокирования)
в связи с тем, что _____ .
_____ (указать причину блокирования персональных данных)

_____ (должность) _____ (подпись) _____ (Ф.И.О.)
" ____ " _____ 20__ г.

Приложение 13
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

В _____
от _____
(Ф.И.О. заявителя)

(наименование и реквизиты
документа, удостоверяющего
личность заявителя)

ЗАЯВЛЕНИЕ

В том случае если Дума Уссурийского городского округа обрабатывает мои персональные данные, прошу предоставить мне сведения о Вашей организации. В противном случае, прошу Вас уведомить меня об отсутствии обработки моих персональных данных.

(должность)

(подпись)

(Ф.И.О.)

"__" _____ 20__ г.

Приложение 14
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

В _____
от _____
(Ф.И.О. заявителя)

(наименование и реквизиты
документа, удостоверяющего
личность заявителя)

ЗАЯВЛЕНИЕ

Прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные, указать цели, способы и сроки ее обработки; предоставить сведения о лицах, которые имеют к ней доступ (которым может быть предоставлен такой доступ); сведения о том, какие юридические последствия для меня может повлечь ее обработка. В случае отсутствия такой информации, прошу Вас уведомить меня об этом.

(должность)

(подпись)

(Ф.И.О.)

"__" _____ 20__ г.

Приложение 15
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

В _____
от _____
(Ф.И.О. заявителя)

(наименование и реквизиты
документа, удостоверяющего
личность заявителя)

ЗАЯВЛЕНИЕ

Прошу уничтожить обрабатываемые Вами мои персональные данные:

(указать уничтожаемые персональные данные)
в связи с тем, что _____.
(указать причину уничтожения персональных данных)

(должность) (подпись) (Ф.И.О.)

" ____ " _____ 20__ г.

Приложение 16
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

В _____
от _____
(Ф.И.О. заявителя)

(наименование и реквизиты
документа, удостоверяющего
личность заявителя)

ЗАЯВЛЕНИЕ

Прошу уточнить обрабатываемые Вами мои персональные данные в соответствии со сведениями: _____;

(указать уточненные персональные данные заявителя)

в связи с тем, что _____.
(указать причину уточнения персональных данных)

(должность)

(подпись)

(Ф.И.О.)

"__" _____ 20__ г.

Приложение 17
к Положению
по обеспечению безопасности
персональных данных в
Думе Уссурийского
городского округа

Согласие
на включение персональных данных в общедоступные источники персональных
данных Думы Уссурийского городского округа

Я, _____,
(Ф.И.О.)
_____ серия _____ N _____,
(вид документа, удостоверяющего личность)
выдан _____,
(когда и кем)
проживающий(ая) по адресу: _____,
_____,
в целях _____
(цель обработки персональных данных)
даю согласие _____
(наименование и адрес оператора)
считать следующие персональные данные общедоступными:

_____.
(перечислить персональные данные)

Согласен на осуществление любых действий (операций) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с моими общедоступными персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение персональных данных, в том числе на передачу, доступ, распространение, предоставление персональных данных определенному кругу лиц.

Настоящее согласие действует со дня его подписания и дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.

Настоящее согласие может быть отозвано в соответствии с законодательством Российской Федерации.

_____ (подпись)
_____ (фамилия, инициалы лица, давшего согласие)
" ____ " _____ г.