УТВЕРЖДЕНА

Приказом
директора административного
департамента аппарата
Администрации Приморского края
от 16.06.2015 №27

ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАТИВНОМ ДЕПАРТАМЕНТЕ АППАРАТА АДМИНИСТРАЦИИ ПРИМОРСКОГО КРАЯ

1. Общие положения

1.1. Настоящая политика в отношении обработки и защиты персональных данных (далее - Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и является основополагающим внутренним документом административного департамента аппарата Администрации Приморского края (далее - Департамент), определяющим ключевые направления деятельности Департамента в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Департамент.

1.2. Положения Политики распространяются на обработку и защиту ПДн, полученных Департаментом как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на обработку и защиту ПДн, полученных до ее утверждения.

1.3. Если в отношениях с Департаментом участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то Департамент является оператором ПДн лиц, представляющих указанные субъекты. Положения Политики и другие внутренние документы Департамента, регулирующие обработку и защиту персональных данных, распространяются на обработку и защиту ПДн наследников (правопреемников) и (или) представителей субъектов ПДн, даже если эти лица в указанных внутренних документах прямо не упоминаются, но фактически участвуют в правоотношениях с Департаментом.

2. Основания обработки и состав персональных данных, обрабатываемых в Департаменте

2.1. Обработка ПДн в Департаменте осуществляется в соответствии с полномочиями Департамента, определяемыми Уставом Приморского края.

2.2. ПДн обрабатываются в Департаменте на основании законодательства Российской Федерации и Приморского края и принятых в соответствии с ними нормативных правовых актов:

2.2.1. Во исполнение Администрацией Приморского края функции регионального оператора ПДн.

2.2.2. В рамках осуществления функции по организации и обеспечению в соответствии с Федеральным законом от 02 мая 2006 года №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» регистрации, централизованного учета и своевременного рассмотрения обращений граждан, направляемых в адрес Администрации Приморского края, Департамента, а также устных обращений граждан.

2.3. Департаментом не ведется обработка специальных категорий персональных данных, а также биометрических персональных данных.

2.4. В целях исполнения возложенных на Департамент функций Департамент в установленном порядке вправе поручить обработку ПДн третьим лицам.

2.5. Департамент предоставляет обрабатываемые им ПДн федеральным органам, исполнительным органам Приморского края и организациям, имеющим в соответствии с федеральным законом право на получение соответствующих ПДн.

2.6. В Департаменте не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Департаменте, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Департаментом ПДн уничтожаются или обезличиваются.

2.7. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Департамент принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Департаменте является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Департамент руководствуется следующими принципами:

1) законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

2) системность: обработка ПДн в Департаменте осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в

информационных системах Департамента (далее - ИС) и других, имеющихся в Департаменте систем и средств защиты;

4) непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

5) своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн принимаются до начала их обработки;

6) преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Департаменте с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

7) персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на гражданских служащих в пределах их обязанностей, связанных с обработкой и защитой ПДн;

8) минимизация прав доступа: доступ к ПДн предоставляется гражданским служащим только в объеме, необходимом для выполнения их должностных обязанностей;

9) гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Департамента (далее - ИСПДн), а также объема и состава обрабатываемых ПДн;

10) открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн Департамента (далее - СЗПДн) не дают возможности преодоления имеющихся в Департаменте систем защиты возможными нарушителями безопасности ПДн;

11) научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

12) специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляются гражданскими служащими, имеющими необходимые для этого квалификацию и опыт;

13) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Департамента предусматривает тщательный подбор персонала и мотивацию гражданских служащих, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;

14) минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Департамента до заключения договоров;

15) наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

16) непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

4. Доступ к обрабатываемым персональным данным

4.1. Доступ к обрабатываемым в Департаменте ПДн имеют лица, уполномоченные приказами директора Департамента, а также лица, чьи ПДн подлежат обработке.

4.2. В целях разграничения полномочий при обработке ПДн полномочия по реализации каждой определенной законодательством функции Департамента закрепляются за соответствующими гражданскими служащими.

4.3. Доступ гражданских служащих к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Департамента. Допуск гражданских служащих к обработке ПДн осуществляется согласно перечню типовых полномочий (ролей пользователей), утверждаемых приказом директора Департамента. Соответствующие полномочия (роль пользователя) вносятся в должностные обязанности указанных гражданских служащих.

4.4. Факты получения доступа к ИСПДн, а также факты обработки ПДн регистрируются, в том числе с использованием средств обеспечения информационной безопасности. Информация о фактах обработки ПДн хранится в Департаменте, включая ИС, в течение установленного срока.

Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Департаментом, осуществляется в соответствии с законодательством Российской Федерации и определяется внутренними регулятивными документами Департамента.

5. Реализация Политики

5.1. Департамент принимает необходимые и достаточные меры для защиты обрабатываемых ПДн от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

5.2. Ответственность за организацию обработки ПДн в Департаменте несут гражданские служащие, назначаемые приказами.

Ответственный за организацию обработки ПДн в Департаменте, в частности, обязан:

1) осуществлять внутренний контроль за соблюдением в Департаменте требований нормативных правовых актов и внутренних регулятивных документов Департамента в области обработки и защиты ПДн;

2) доводить до сведения гражданских служащих положения нормативных правовых актов и внутренних регулятивных документов в области обработки и защиты ПДн;

3) организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.3. Департамент осуществляет обработку ПДн без использования средств автоматизации, а также с использованием таких средств.

5.4. При обработке ПДн без использования средств автоматизации Департамент в соответствии с положениями нормативных правовых актов в области обработки и защиты ПДн реализует комплекс организационных и технических мер, обеспечивающих:

обособление ПДн от информации, не содержащей ПДн;

раздельную обработку и хранение каждой категории ПДн (фиксация на отдельных материальных носителях ПДн, цели обработки которых заведомо несовместимы);

соответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн установленным требованиям;

соблюдение установленных требований при ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн в помещения Департамента, или в иных аналогичных целях;

сохранность материальных носителей ПДн;

условия хранения, исключающие несанкционированный доступ к ПДн, а также смешение ПДн (материальных носителей), обработка которых осуществляется в различных целях;

надлежащее уточнение, уничтожение или обезличивание ПДн.

5.5. В соответствии с требованиями нормативных правовых актов в области обработки и защиты ПДн, обработки ПДн с использованием средств автоматизации в Департаменте используются ИСПДн.

Все ИСПДн принимаются в эксплуатацию после прохождения периодической классификации и аттестации в соответствии с требованиями нормативных правовых актов в области обеспечения безопасности ПДн.

Для каждой ИСПДн должна предоставляться модель угроз безопасности ПДн, на основе которой проводятся мероприятия по обеспечению безопасности информации в соответствии с требованиями, предъявляемыми к установленному классу ИСПДн.

Устанавливаются следующие требования к периодичности пересмотра моделей угроз для каждой ИСПДн:

в плановом порядке для существующих ИСПДн - ежегодно;

в случае существенных изменений в инфраструктуре или порядке обработки ПДн в ИСПДн - в течение трех месяцев с даты фиксации изменений;

в случае создания новой ИСПДн (выделения части из существующей ИСПДн) - в течение одного месяца с даты создания (выделения) ИСПДн.

5.6. Обработка ПДн в Департаменте с использованием средств автоматизации ведется только в ИСПДн. В Департамента запрещается обработка ПДн с целями, не соответствующими целям создания ИСПДн, эксплуатация ИСПДн в составе, отличном от указанного при создании ИСПДн.

5.7. Ввод в эксплуатацию ИСПДн оформляется актом ввода в эксплуатацию и на основе аттестации ИСПДн или декларирования соответствия ИСПДн требованиям по безопасности ПДн.

5.8. В целях обеспечения управления информационной безопасностью ПДн в Департаменте используется СЗПДн.

Объектами защиты СЗПДн являются информация, обрабатываемая Департаментом и содержащая ПДн, а также инфраструктура, содержащая и поддерживающая указанную информацию.

5.9. СЗПДн реализуется комплексом правовых, режимных, организационных и программно-технических мер, которые включают:

подготовку внутренних регулятивных документов Департаменте по вопросам обработки и защиты ПДн, контроль за исполнением в Департаменте требований нормативных правовых актов и внутренних регулятивных документов Департаменте в области обработки и защиты ПДн, а также внесение соответствующих изменений в имеющиеся внутренние регулятивные документы;

оформление письменных обязательств гражданских служащих о неразглашении ПДн;

доведение до сведения гражданских служащих информации об установленных законодательством Российской Федерации санкциях за нарушения, связанные с обработкой и защитой ПДн;

обеспечение наличия в положениях о структурных подразделениях Департамента и должностных обязанностях требований по соблюдению установленного порядка обработки и защиты ПДн;

разработку и введение в действие внутренних регулятивных документов Департаменте по обеспечению информационной безопасности ИСПДн;

регламентацию процедур создания и осуществление документирования действующих инженерных и информационных систем, программных комплексов, порядка внесения в них изменений и своевременной актуализации эксплуатационной документации;

ознакомление гражданских служащих с положениями нормативных правовых актов и внутренних регулятивных документов Департамента в области обработки и защиты ПДн и (или) организация обучения их правилам обработки и защиты ПДн;

проведение мероприятий по регламентации, установлению, поддержанию и осуществлению контроля за состоянием:

физической охраны, контрольно-пропускного режима, перемещением технических средств и носителей информации;

защиты технологических процессов, информационных ресурсов, информации и поддерживающей их инфраструктуры от угроз техногенного характера и внешних неинформационных воздействий;

регламентацию обработки ПДн, в том числе хранения и передачи информации как внутри Департамента, так и при взаимодействии с контрагентами Департамента, органами и организациями, обращения с документами (включая электронные документы) и носителями, порядка их учета, хранения и уничтожения;

установление правил доступа на объекты, в помещения, в ИС, применение в этих целях систем охраны и управления доступом.

осуществление контроля эффективности организационных мер защиты;

разработку защитных технических решений:

при стратегическом планировании архитектуры ИС;

выборе технических средств обработки информации;

разработке и (или) приобретении программного обеспечения;

13) применение следующих компонентов программно-технических мер защиты:

защищенных средств (систем) обработки информации, содержащей ПДн;

системы криптографической защиты информации при ее передаче по каналам связи;

межсетевых экранов для логического разделения подсетей и защиты от несанкционированного доступа из внешних (открытых) информационных систем;

аппаратных и программных средств защиты и контроля, устройств, технических систем и средств, используемых для обеспечения информационной безопасности, в том числе для обнаружения и нейтрализации попыток несанкционированного доступа к информации.

5.10. Для всех критичных в отношении обеспечения целостности и доступности ПДн функций ИСПДн используются соответствующие планы обеспечения непрерывной работы и восстановления при авариях и стихийных бедствиях, которые не реже одного раза в квартал подлежат актуализации. Гражданские служащие проходят обучение необходимым действиям по обеспечению целостности и доступности ПДн в нештатных ситуациях.

6. Основные мероприятия по обеспечению безопасности персональных данных

6.1. Мероприятия по защите ПДн реализуются в Департаменте уполномоченными органами, гражданскими служащими в следующих направлениях:

предотвращение утечки информации, содержащей ПДн, по техническим каналам связи и иными способами;

предотвращение несанкционированного доступа к содержащей ПДн информации, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

защита от вредоносных программ;

обеспечение безопасного межсетевого взаимодействия;

обеспечение безопасного доступа к сетям международного информационного обмена;

анализ защищенности ИСПДн;

обеспечение защиты информации с использованием шифровальных (криптографических) средств при передаче ПДн по каналам связи;

обнаружение вторжений и компьютерных атак;

осуществление контроля за реализацией системы защиты ПДн.

6.2. Мероприятия по обеспечению безопасности ПДн включают в себя:

реализацию разрешительной системы допуска пользователей к информационным ресурсам информационных систем (далее - ИС) и связанным с их использованием работам, документам;

разграничение доступа пользователей ИСПДн и обслуживающих ИСПДн специалистов к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

регистрацию действий пользователей и обслуживающих ИСПДн специалистов, контроль несанкционированного доступа и действий пользователей и обслуживающих специалистов, а также третьих лиц;

использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

предотвращение внедрения в ИС вредоносных программ и программных закладок, анализ принимаемой по информационно-телекоммуникационным сетям (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов;

ограничение доступа в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации, содержащие ПДн;

размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку ПДн;

учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

резервирование технических средств, дублирование массивов и носителей информации;

реализацию требований по безопасному межсетевому взаимодействию ИС;

использование защищенных каналов связи, защиту информации при ее передаче по каналам связи;

межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры ИС;

обнаружение вторжений в ИС, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на ИС;

активный аудит безопасности ИС на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;

анализ защищенности ИС с применением специализированных программных средств (сканеров безопасности);

централизованное управление системой защиты ПДн в ИС.

6.3. В целях осуществления внутреннего контроля в Департаменте проводятся периодические проверки условий обработки ПДн. Такие проверки осуществляются ответственным за организацию обработки ПДн в Департаменте.