АДМИНИСТРАЦИЯ
ГОРОДСКОГО ОКРУГА ЩЁЛКОВО

РАСПОРЯЖЕНИЕ

от 18.12.2020 № 340-р
г. Щёлково, Московская область

Об утверждении и вводе в
действие комплекта документации,
регламентирующей обработку и
защиту персональных данных

Во исполнение требований Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Постановления 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»; Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; нормативно-методических документов Федеральной службы по техническому и экспортному контролю России и Федеральной службы безопасности России,

002525

1. Считать утвержденным с 18 декабря 2020 года следующий прилагаемый комплект документации:

– инструкция администратора безопасности;

– инструкция администратора ИС;

– форма журнала применяемых средств защиты информации, эксплуатационной и технической документации к ним;

– форма журнала учета машинных носителей информации;

– форма журнала учета мероприятий по контролю обеспечения защиты информации;

– инструкция ответственного за организацию обработки персональных данных;

– форма журнала учета обращений субъектов персональных данных о выполнении их законных прав, при обработке данных в информационных системах;

– инструкция по антивирусной защите;

– инструкция по организации парольной защиты;

– инструкция по работе со средствами криптографической защиты информации;

– форма журнала учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов;

– форма лицевого счета пользователя средств криптографической защиты информации;

– инструкция по ведению журналов;

– инструкция пользователей в части обеспечения безопасности персональных данных при их обработке в информационных системах;

– положение о порядке учета, хранения и уничтожения носителей персональных данных;

– форма акта уничтожения носителей персональных данных;

– форма акта уничтожения персональных данных с машинного носителя;

– положение по обработке персональных данных, осуществляемой без использования средств автоматизации;

– порядок доступа в помещения, где осуществляется работа с персональными данными, и организация режима безопасности в этих помещениях;

– перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн «Кадры», необходим для выполнения служебных обязанностей;

– перечень лиц, допущенных к работе со средствами криптографической защиты информации;

– матрица разграничения доступа к ресурсам ИСПДн «Кадры»;

– порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, защищаемой информации и средств защиты;

– правила обработки персональных данных;

– правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

– форма акта проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

– план мероприятий по защите информации в ИС;

– правила работы с обезличенными данными в случае обезличивания персональных данных;

– перечень должностей служащих, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных;

– перечень должностей служащих, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

– перечень информационных систем Администрации городского округа Щёлково;

– перечень персональных данных, подлежащих защите в Администрации городского округа Щёлково;

– регламент технологического процесса обработки защищаемой информации в ИСПДн «Кадры»;

– правила рассмотрения запросов субъектов персональных данных или их представителей;

– формы запросов, разъяснений, отказов, связанных с рассмотрением запросов субъектов персональных данных или их представителей;

– форма типового обязательство сотрудника Администрации городского округа Щёлково о прекращении обработки персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, в случае увольнения или перехода на должность, не предусматривающую доступ к персональным данным;

– форма соглашения о неразглашении персональных данных;

– форма согласия на обработку персональных данных;

– форма разъяснения юридических последствий отказа предоставить свои персональные данные;

– политика в отношении обработки персональных данных.

2. Назначить ответственным за исполнение настоящего распоряжения начальника Административного управления Администрации городского округа Щёлково Вершинина А.О.

3. Контроль за исполнением настоящего распоряжения оставляю за собой.

Глава
Городского округа Щёлково А.А. Булгаков

Администрация городского округа Щёлково
Административное управление

КОПИЯ ВЕРНА
Начальник общего отдела
Административного управления
С. А. Родионова
(подпись ответственного лица)

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

ФОРМА
Журнал учета мероприятий по контролю обеспечения защиты информации

Журнал начат: «_____» _____ 20____г.

Должность: _____

_____/Ф. И. О. должностного лица/

Журнал окончен: «_____» _____20____г.

Должность: _____

_____/Ф. И. О. должностного лица/

На _____листах

Щёлково 20__

№	Мероприятие	Дата	Исполнитель	Результат

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Инструкция
ответственного за организацию обработки персональных данных

I. Общие положения

1.1. Ответственный за организацию обработки персональных данных назначается распоряжением Администрации городского округа Щёлково.

1.2. Ответственный за организацию обработки персональных данных подчиняется главе городского округа Щёлково.

1.3. Ответственный за организацию обработки персональных данных в своей работе руководствуется настоящей инструкцией, Политикой в отношении обработки персональных данных, руководящими и нормативными документами ФСТЭК России и ФСБ России, а также иными регламентирующими документами Оператора (Оператор – Администрация городского округа Щёлково).

1.4. Ответственный за организацию обработки персональных данных отвечает за методическое и нормативное обеспечение пользователей информационных систем (далее – ИС), контроль работоспособности всех элементов ИС при обработке персональных данных (далее – ПДн).

1.5. Ответственный за организацию обработки персональных данных является лицом, уполномоченным на проведение работ по контролю и анализу, а также по технической поддержке технических и программных средств обработки и хранения ПДн в ИС.

1.6. Ответственный за организацию обработки персональных данных должен иметь специальное рабочее место, размещенное в здании Оператора так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. Ответственный за организацию обработки персональных данных осуществляет методическое руководство всех пользователей в вопросах безопасной обработки и хранения ПДн.

1.8. Требования ответственного за организацию обработки персональных данных, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения администратором ИС и всеми пользователями ИС.

1.9. Ответственный за организацию обработки персональных данных несет персональную ответственность за качество проводимых им работ по контролю работоспособности всех элементов ИС.

II. Должностные обязанности

Ответственный за организацию обработки персональных данных обязан:

2.1. Знать и выполнять требования действующих законодательных и нормативных правовых актов, регламентирующих деятельность юридических лиц в сфере обработки ПДн; локальных правовых актов, регламентирующих деятельность Оператора по обработке и защите ПДн; локальных правовых актов Оператора, регламентирующих правила и нормы охраны труда, техники безопасности и противопожарной безопасности; настоящей инструкции.

2.2. Осуществлять контроль учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.3. Осуществлять контроль работоспособности средств обработки и хранения информации.

2.4. Реагировать на инциденты, приведшие к отказу работоспособности, принимать решения по устранению неполадок, приведших к нарушению работоспособности ИС.

2.5. Требовать у руководства прекращения обработки информации, как в целом, так и для отдельных пользователей ИС, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИС или средств защиты.

2.6. Принимать решение о временной блокировке пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИС или средств защиты.

2.7. Принимать решения о необходимости привлечения сторонних лиц для технического обслуживания элементов ИС, присутствовать лично, или назначать сопровождающим администратора ИС, при выполнении такого технического обслуживания.

2.8. Контролировать порядок работы пользователей ИС.

2.9. Контролировать выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт.

2.10. Контролировать работы по внедрению программных средств.

2.11. В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям организовывать проведение периодических проверок условий обработки ПДн.

2.12.Доводить до операторов ИС требования по защите ПДн, а также положения организационно-распорядительных документов по защите ПДн с учетом внесенных в них изменений.

2.13.О результатах проводимых проверок и мерах, необходимых для устранения выявленных нарушений, докладывать руководству.

2.14.Анализировать изменения угроз безопасности и оценивать возможные последствия реализации угроз безопасности в ИС, принимать меры защиты ПДн в случае возникновения новых угроз безопасности информации.

2.15.Принимать участие в актуализации/доработке организационно-распорядительных документов, регламентирующих обработку и защиту информации в рамках своей компетенции.

2.16.Осуществлять ознакомление операторов ИС, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн (в том числе с требованиями к защите ПДн), локальными правовыми актами по вопросам обработки ПДн и (или) организовывать обучение указанных лиц.

2.17.Организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.18.Уведомлять уполномоченный орган за обеспечение защиты прав субъектов ПДн об обработке (намерении осуществлять обработку) персональных данных, за исключением случаев, установленных Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных».

III. Права Ответственного за организацию обработки персональных данных

Ответственный за организацию обработки персональных данных имеет право:

3.1.Запрещать устанавливать на рабочих станциях нештатное программное и аппаратное обеспечение.

3.2.Требовать от пользователей выполнения инструкций в части работы с программными, аппаратными средствами, средствами защиты и ПДн.

3.3.Блокировать доступ к защищаемой информации любых пользователей, если это необходимо для предотвращения нарушения режима защиты.

3.4.Проводить внеплановые проверки соблюдения установленного режима обработки и защиты информации.

3.5.Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности.

3.6.Представлять руководству предложения по совершенствованию мер защиты.

IV. Ответственность Ответственного за организацию обработки персональных данных

Ответственный за организацию обработки персональных данных несет ответственность:

4.1. За невыполнение и/или несвоевременное, халатное выполнение своих должностных обязанностей.

4.2. За несоблюдение действующих инструкций, положений и приказов по сохранению конфиденциальности персональных данных.

4.3. За нарушение правил внутреннего трудового распорядка, трудовой дисциплины, правил техники безопасности и противопожарной безопасности.

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданско-правовую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Инструкция
по антивирусной защите

I. Общие положения

1. Настоящая Инструкция определяет требования к организации антивирусной защиты в информационных системах (далее – ИС) Администрации городского округа Щёлково (далее – Оператор).

2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

3. Настоящая Инструкция предназначена для пользователей, осуществляющих обработку информации в ИС, администратора безопасности и иных уполномоченных лиц.

4. Защита от вредоносного программного обеспечения осуществляется путем применения специализированных средств антивирусной защиты.

5. Организация работ по антивирусной защите и ответственность за сопровождение подсистемы антивирусной защиты возлагается на администратора безопасности.

6. К применению в ИС допускаются только лицензионные средства антивирусной защиты.

7. Программное обеспечение антивирусной защиты устанавливается на все средства вычислительной техники, входящие в состав ИС.

8. Антивирусная программа должна запускаться при старте операционной системы и функционировать в течение всего времени работы пользователя на компьютере.

9. Периодически в установленное время в автоматическом режиме должен проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов.

10. Должно осуществляться периодическое обновление антивирусных пакетов и контроль их работоспособности.

11. Администратор безопасности должен проводить периодическое тестирование всего установленного программного обеспечения на предмет наличия программных вирусов.

12. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые

файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.

13. Контроль входящей информации необходимо проводить непосредственно после ее приема.

14. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

15. При работе с отчуждаемыми носителями информации пользователи обязаны перед началом работы осуществить проверку носителя на предмет отсутствия компьютерных вирусов.

16. При обнаружении компьютерного вируса пользователь ИС обязан немедленно поставить в известность администратора безопасности и прекратить работу в ИС.

17. Администратор безопасности проводит в случае необходимости лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

18. В случае обнаружения на отчуждаемом носителе нового вируса, не поддающегося лечению, администратор безопасности обязан запретить использование носителя.

19. В случае обнаружения на накопителе на жестком магнитном диске не поддающегося лечению вируса, администратор безопасности обязан запретить работу в ИС и в возможно короткие сроки обновить пакет антивирусных программ.

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Инструкция
администратора безопасности

I. Общие положения

1.1. Администратор безопасности назначается распоряжением Администрации городского округа Щёлково.

1.2. Администратор безопасности подчиняется ответственному за организацию обработки персональных данных и согласует свои действия с ним.

2.1.Администратор безопасности в своей работе руководствуется настоящей инструкцией, Политикой в отношении обработки персональных данных, руководящими и нормативными документами ФСТЭК России и ФСБ России, а также иными регламентирующими документами Оператора (Оператор – Администрация городского округа Щёлково).

1.3. Администратор отвечает за поддержание необходимого уровня безопасности объектов защиты.

1.4. Администратор безопасности является ответственным лицом Оператора, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты информационной системы (далее – ИС) и ее(их) ресурсов на этапах промышленной эксплуатации и модернизации.

1.5. Администратор безопасности является уполномоченным на проведение работ по управлению (администрированию) системой защиты информации, конфигурацией ИС и конфигурацией ее системы защиты.

1.6. Администратор безопасности должен иметь специальное рабочее место, размещенное в здании Оператора так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), а также средствами контроля за техническими средствами обработки и хранения ПДн (при необходимости).

1.8. Администратор безопасности осуществляет методическое руководство операторов ИС и администратора ИС в вопросах обеспечения безопасности персональных данных.

1.9. Требования Администратора безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИС.

1.10.Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИС, состояние и поддержание установленного уровня защиты каждой ИС.

II. Должностные обязанности

Администратор безопасности обязан:

2.1. Знать и выполнять требования действующих законодательных и нормативных правовых актов, регламентирующих деятельность юридических лиц в сфере обработки персональных данных; внутренних локальных нормативных актов, регламентирующих деятельность Оператора по обработке и защите персональных данных; локальных нормативных актов Оператора, регламентирующих правила и нормы охраны труда, техники безопасности и противопожарной безопасности; настоящей инструкции.

2.2. Осуществлять установку, настройку и обновление средств защиты.

2.3. Совместно с Администратором ИС обеспечивать доступ к защищаемой информации пользователям ИС согласно их правам доступа, а также поддерживать в актуальном состоянии правила разграничения доступа.

2.4. Обеспечивать функционирование системы защиты ИС в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов.

2.5. Анализировать состояние защиты ИС и ее(их) отдельных подсистем.

2.6. Контролировать неизменность параметров и режимов работы средств защиты.

2.7. Контролировать физическую сохранность средств и оборудования ИС.

2.8. Совместно с Администратором ИС выявлять, анализировать и устранять уязвимости и иные недостатки в функционировании системы защиты информации ИС.

2.9. Контролировать пользователей ИС на предмет правильности работы с техническими элементами ИС и средствами защиты информации.

2.10.Осуществлять мониторинг и анализ зарегистрированных событий в ИС, связанных с обеспечением безопасности, в том числе анализ журналов учета событий, регистрируемых средствами защиты.

2.11.Своевременно реагировать на инциденты информационной безопасности, обеспечивая сбор необходимых данных для проведения расследования.

2.12.Совместно с Администратором ИС не допускать установку, использование, хранение и размножение в ИС программных средств, не связанных с выполнением функциональных задач.

2.13.Совместно с Администратором ИС не допускать к работе на элементах ИС посторонних лиц.

2.14.Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИС.

2.15.Оказывать помощь пользователям ИС в части применения средств защиты и консультировать по вопросам введенного режима защиты.

2.16.Осуществлять информирование пользователей ИС о появлении актуальных угроз безопасности, о правилах безопасной эксплуатации ИС.

2.17.Проводить обучение пользователей ИС правилам эксплуатации отдельных средств защиты, в том числе проведение практических занятий и тренировок с персоналом ИС по блокированию угроз безопасности информации и реагированию на инциденты.

2.18.Принимать участие в актуализации/доработке организационно-распорядительных документов, регламентирующих обработку и защиту информации в рамках своей компетенции.

2.19.В случае отказа работоспособности технических средств и средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности. В случае невозможности своевременно устранить причины, приведшие к отказу работоспособности, Администратор безопасности обязан доложить о случившемся инциденте ответственному за организацию обработки персональных данных.

2.20.Вести Журналы, необходимые для выполнения требований законодательства РФ в сфере обработки и защиты информации в соответствии с организационно-распорядительной документацией Оператора.

III. Права администратора безопасности

Администратор безопасности имеет право:

3.1. Отключать от сети пользователей, осуществивших НСД к защищаемым ресурсам ИС или нарушивших другие требования по безопасности информации.

3.2. Участвовать в любых проверках ИС.

3.3. Запрещать устанавливать на серверах и рабочих станциях ИС нештатное программное и аппаратное обеспечение.

3.4. Представлять руководству предложения по совершенствованию мер защиты.

IV. Ответственность администратора безопасности

Администратор несет ответственность:

4.1. За невыполнение и/или несвоевременное, халатное выполнение своих должностных обязанностей.

4.2. За несоблюдение действующих инструкций, положений и приказов по сохранению конфиденциальности персональных данных.

4.3. За нарушение правил внутреннего трудового распорядка, трудовой дисциплины, правил техники безопасности и противопожарной безопасности.

4.4. За все действия, совершенные от имени его учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетной записи.

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданско-правовую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Инструкция
администратора ИС

I. Общие положения

1.1. Администратор информационной(ых) систем(ы) (далее – Администратор ИС) назначается распоряжением Администрации городского округа Щёлково.

1.1. Администратор ИС подчиняется ответственному за организацию обработки персональных данных и согласует свои действия с ним.

1.2. Администратор ИС в своей работе руководствуется настоящей инструкцией, Политикой в отношении обработки персональных данных, руководящими и нормативными документами ФСТЭК России и ФСБ России, а также иными регламентирующими документами Оператора (Оператор – Администрация городского округа Щёлково).

1.3. Администратор ИС отвечает за обеспечение стабильной работы всех элементов информационной(ых) систем(ы) (далее – ИС) при обработке персональных данных (далее – ПДн).

1.4. Администратор ИС является ответственным лицом Оператора, уполномоченным на проведение работ по технической поддержке аппаратных и программных средств обработки и хранения ПДн в ИС.

1.5. Администратор ИС должен иметь специальное рабочее место, размещенное в здании Оператора так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.6. Рабочее место Администратора ИС должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), а также средствами контроля за техническими средствами обработки и хранения ПДн (при необходимости).

1.7. Администратор ИС осуществляет методическое руководство операторов ИС в вопросах безопасной обработки и хранения ПДн.

1.8. Требования Администратора ИС, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИС.

1.9. Администратор ИС несет персональную ответственность за качество проводимых им работ по обеспечению стабильной работы операторов в ИС.

II. Должностные обязанности

Администратор ИС обязан:

2.1. Знать и выполнять требования действующих законодательных и нормативных правовых актов, регламентирующих деятельность юридических лиц в сфере обработки персональных данных; внутренних локальных нормативных актов, регламентирующих деятельность Оператора по обработке и защите персональных данных; локальных нормативных актов Оператора, регламентирующих правила и нормы охраны труда, техники безопасности и противопожарной безопасности; настоящей инструкции.

2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИС (за исключением средств защиты информации) с учетом особенностей функционирования ИС. К элементам ИС относятся в том числе:

– программное обеспечение (операционные системы, прикладное и специальное программное обеспечение);

– программно-аппаратные средства.

2.3. Обеспечивать работоспособность элементов ИС и локальной вычислительной сети Оператора.

2.4. Осуществлять учет, создание, хранение и использование резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5. Обеспечивать функционирование и поддерживать работоспособность средств обработки и хранения информации.

2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИС, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности. В случае невозможности своевременно устранить причины, приведшие к отказу работоспособности, Администратор ИС обязан доложить о случившемся инциденте ответственному за организацию обработки персональных данных.

2.7. Совместно с Администратором безопасности проводить периодический контроль принятых мер по защите ПДн.

2.8. Осуществлять управление учетными записями пользователей.

2.9. Хранить, осуществлять выдачу персональных паролей операторов ИС, осуществлять контроль над правильностью использования персонального пароля пользователями ИС.

2.10.Выявлять нарушения установленного порядка работ или нарушения функционирования ИС или средств защиты и докладывать обо всех нарушениях ответственному за организацию обработки персональных данных.

2.11.Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств

и отправке их в ремонт. Техническое обслуживание криптографических средств защиты информации должно проводиться организациями, имеющими соответствующие лицензии.

2.12.При необходимости, по согласованию с ответственным за организацию обработки персональных данных, привлекать сторонних лиц для технического обслуживания элементов ИС, присутствовать при выполнении такого технического обслуживания.

2.13.Совместно с Администратором безопасности принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий. В случае невозможности своевременно ликвидировать последствия аварийных и внештатных ситуаций, Администратор ИС обязан доложить о возникшем инциденте ответственному за организацию обработки персональных данных.

2.14.Совместно с Администратором безопасности выявлять, анализировать и устранять уязвимости и иные недостатки в функционировании системы защиты информации ИС.

2.15.Поддерживать в актуальном рабочем состоянии полный объем оперативной и накапливаемой информации.

2.16.Анализировать информационные потребности структурных подразделений Оператора.

2.17.Осваивать программные средства, использующиеся сотрудниками Оператора.

2.18.Согласовывать с ответственным за организацию обработки персональных данных вопросы по совершенствованию процесса хранения и обработки информации с целью обеспечения требуемой достоверности результатов и минимизации времени расчетов.

2.19.Обеспечивать обмен информацией в соответствии с установленным порядком (в том числе с использованием электронных сетей телекоммуникаций).

2.20.Осуществлять комплекс работ по внедрению программных средств, за исключением средств защиты информации.

2.21.Осуществлять контроль работы компьютеров и своевременно сообщать о сбоях и неисправностях ответственному за организацию обработки персональных данных.

2.22. Осуществлять учет и хранение документов, имеющих отношение к автоматизированной обработке информации на компьютерах.

2.23. Обобщать и анализировать замечания пользователей по результатам эксплуатации задач и передавать информацию об отмеченных недостатках руководству.

2.24.Следить за обеспечением целостности, доступности и конфиденциальности циркулирующих в ИС персональных данных.

2.25.Вести архив используемых программных средств и нормативно-справочной информации.

2.26.Принимать участие в актуализации/доработке организационно-распорядительных документов, регламентирующих обработку и защиту информации в рамках своей компетенции.

2.27.Вести Журналы, необходимые для выполнения требований законодательства РФ в сфере обработки и защиты информации в соответствии с организационно-распорядительной документацией Оператора.

III. Права Администратора ИС

Администратор ИС имеет право:

3.1. Запрещать устанавливать на рабочих станциях нештатное программное и аппаратное обеспечение.

3.2. Требовать от пользователей выполнения инструкций в части работы с программными, аппаратными средствами и персональными данными.

3.3. Блокировать доступ к защищаемой информации любых пользователей, если это необходимо для предотвращения нарушения режима защиты.

3.4. Представлять руководству предложения по совершенствованию мер защиты.

IV. Ответственность Администратора ИС

Администратор ИС несет ответственность:

4.1. За невыполнение и/или несвоевременное, халатное выполнение своих должностных обязанностей.

4.2. За несоблюдение действующих инструкций, положений и приказов по сохранению конфиденциальности персональных данных.

4.3. За нарушение правил внутреннего трудового распорядка, трудовой дисциплины, правил техники безопасности и противопожарной безопасности.

4.4. За все действия, совершенные от имени его учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетной записи.

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданско-правовую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой

информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Инструкция
по организации парольной защиты

I. Общие положения

1.1.Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах (далее – ИС) Администрации городского округа Щёлково (далее – Оператор).

1.2.Настоящая Инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

1.3.Настоящая Инструкция предназначена для пользователей, осуществляющих обработку информации в ИС, администратора ИС и иных уполномоченных лиц.

1.4.Пользователем является каждый сотрудник Оператора, участвующий в рамках своих функциональных обязанностей в процессах обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.5.Пользователь несет персональную ответственность за свои действия.

1.6.Методическое руководство работой пользователя осуществляется администратором ИС и администратором безопасности.

II. Организация парольной защиты

2.1. Личные пароли доступа к элементам ИС выдаются пользователям администратором ИС.

2.2. Правила формирования пароля:

– пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

– пароль должен состоять не менее чем из 6 символов;

– в пароле должны присутствовать символы следующих категорий:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

– запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

– запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

– запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;

– запрещается выбирать пароли, которые уже использовались ранее.

2.3. В ИС должна быть осуществлена защита аутентификационной информации в процессе ее ввода от возможного использования лицами, не имеющими на это полномочий. Защита обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «*», «•» или иными знаками.

2.4. Количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя должно быть не более 5. Разблокирование учетной записи осуществляется администратором ИС.

2.5. После 10 минут бездействия (неактивности) пользователя должно происходить автоматическое блокирование сеанса доступа. Блокирование сеанса доступа пользователя в информационную систему должно сохраняться до прохождения им повторной идентификации и аутентификации.

2.6. Порядок смены паролей:

– полная плановая смена паролей пользователей в ИС должна проводиться регулярно, не реже одного раза в 3 месяца;

– полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий администратора ИС, которым по роду службы были предоставлены полномочия по управлению парольной зашитой;

– полная внеплановая смена паролей должна производиться в случае компрометации личного пароля администратора ИС или администратора безопасности;

– в случае компрометации личного пароля пользователя, надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

2.7. Правила ввода пароля:

– ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

– во время ввода паролей необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами или техническими средствами (видеокамерами и др.).

2.8. Правила хранения пароля:

– запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

– запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем;

– хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля, сейфе, либо в сейфе у администратора ИС или администратора безопасности.

2.9. Лица, использующие паролирование, обязаны:

– четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

– своевременно сообщать ответственным лицам об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

ФОРМА

Журнал учета обращений субъектов персональных данных о выполнении их законных прав, при обработке данных в информационных системах

Журнал начат: «_____» _____ 20____г.

Должность: _____

_____/Ф. И. О. должностного лица/

Журнал окончен: «_____» _____20____г.

Должность: _____

_____/Ф.И.О. должностного лица/

На _____листах

Щёлково 20__

№	ФИО	Дата обращения	Регистрационный № запроса	Цель обращения	Результат

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

ФОРМА

Журнал учета применяемых средств защиты информации, эксплуатационной и технической документации к ним

Журнал начат: «_____» _____ 20____г.

Должность: _____

_____/Ф. И. О. должностного лица/

Журнал окончен: «_____» _____20____г.

Должность: _____

_____/Ф.И.О. должностного лица/

На _____листах

Щёлково 20__

№	Наименование СЗИ	Регистрационный № СЗИ, эксплуатационной и технической документации к ним / номер экземпляра	Отметка о получении		Отметка о подключении (установке) СЗИ			Примечание
			От кого получены	Дата и № сопроводительных документов	ФИО лица, производившего подключение (установку)	Дата установки и подпись	№ аппаратных средств, в которые установлены или к которым подключены СЗИ	

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

ФОРМА
Журнал учета машинных носителей информации

Журнал начат: «_____» _____ 20____г.

Должность: _____

_____/Ф. И. О. должностного лица/

Журнал окончен: «_____» _____20____г.

Должность: _____

_____/Ф.И.О. должностного лица/

На _____листах

Щёлково 20__

№	Тип, емкость носителя	Заводской (учетный) номер	Отметка о выдаче		Отметка о возврате		Отметка об уничтожении	Примечание
			ФИО пользователя	Дата и подпись	ФИО пользователя	Дата и подпись		
1.								
2.								
3.								
4.								
5.								
6.								

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Инструкция
по работе со средствами криптографической защиты информации

I. Организация и обеспечение безопасности обработки с использованием шифровальных (криптографических) средств

1.1. Обеспечение функционирования и безопасности средств криптографической защиты информации (далее – криптосредства) возлагается на ответственного пользователя средств криптографической защиты информации, имеющего необходимый уровень квалификации, и назначается распоряжением Администрации городского округа Щёлково.

1.2. Допускается возложение функций ответственного пользователя средств криптографической защиты информации на:

– одного из пользователей криптосредств;

– на структурное подразделение или должностное лицо (сотрудника) Администрации городского округа Щёлково (далее – Оператор).

1.3. Пользователи криптосредств должны учитывать, что безопасность обработки с использованием криптосредств обеспечивается:

– соблюдением пользователями криптосредств, конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документов к ним;

– точным выполнением пользователями криптосредств, требований к обеспечению безопасности информации;

– надежным хранением эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

– своевременным выявлением попыток посторонних лиц получить сведения о защищаемой информации, об используемых криптосредствах или ключевых документов к ним;

– немедленным принятием мер по предупреждению разглашения защищаемой информации, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

1.4. Лица, оформляемые на работу в качестве пользователей криптосредств, должны быть ознакомлены с настоящей Инструкцией и другими документами, регламентирующими организацию и обеспечение безопасности информации при их обработке в информационной системе, под личную подпись и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

1.5. Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на ответственного пользователя средств криптографической защиты информации в пределах его служебных полномочий.

II. Порядок обращения с криптосредствами и криптоключами к ним. Мероприятия при компрометации криптоключей

2.1 Ответственный пользователь средств криптографической защиты информации осуществляет ведение Журнала учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов. В журнале регистрируются числящиеся за пользователями криптосредств, эксплуатационная и техническая документация к ним, ключевые документы.

2.2 Ответственный пользователь средств криптографической защиты информации заводит и ведет на каждого пользователя средств криптографической защиты информации лицевой счет, в котором регистрирует числящиеся за конкретным пользователем средства криптографической защиты информации, эксплуатационную и техническую документацию к ним, ключевые документы.

2.3 Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и (или) ответственным пользователем средств криптографической защиты информации под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована ответственным пользователем средств криптографической защиты информации.

2.4 Криптосредства и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или ответственными пользователями криптосредств и сотрудниками при соблюдении мер, исключающих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки.

2.5 Эксплуатационную и техническую документацию к криптосредствам можно пересылать заказными или ценными почтовыми отправлениями.

2.6 Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов следует производить заблаговременно. Указание о вводе в действие очередных ключевых документов может быть дано ответственным пользователем средств криптографической защиты информации, только после поступления от всех заинтересованных пользователей криптосредств подтверждения о получении ими очередных ключевых документов.

2.7 Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному пользователю средств криптографической защиты информации или по его указанию должны быть уничтожены на месте.

2.8 Ключевые документы уничтожаются либо пользователями криптосредств, либо ответственным пользователем средств криптографической защиты информации под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи криптосредств должны уведомить об этом ответственного пользователя средств криптографической защиты информации для списания уничтоженных документов.

2.9 Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного пользователя средств криптографической защиты информации, согласованного с руководством Оператора, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

2.10 О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации, пользователи криптосредств обязаны сообщать ответственному пользователю средств криптографической защиты информации и (или) руководству Оператора.

2.11 Изготовлять ключевые документы из исходной ключевой информации могут операторы ИС или ответственные пользователи средств криптографической защиты информации, применяя штатные криптосредства, если такая возможность предусмотрена эксплуатационной и технической документацией к криптосредствам.

III. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним

3.1. Ответственный пользователь средств криптографической защиты информации устанавливает режим охраны помещений, где установлены криптосредства или хранятся ключевые документы к ним (далее – Помещения).

3.2. Помещения должны быть оснащены входными дверьми с замками, организовано обеспечение постоянного закрытия дверей Помещений на замок и их открытие только для санкционированного прохода, а также опечатывание Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений.

3.3. Доступ в Помещения в рабочее время имеют сотрудники, включенные в Перечень лиц, имеющих право самостоятельного доступа в помещения, в которых размещены средства криптографической защиты информации (далее – Перечень).

3.4. В нерабочее время пребывание вышеуказанных сотрудников разрешается на основании служебных записок (или иных видов разрешающих документов).

3.5. Нахождение в Помещениях посторонних лиц в рабочее время разрешается только в присутствии сотрудников, включенных в Перечень. В нерабочее время нахождение в Помещениях посторонних лиц запрещается.

3.6. Сотрудники органов МЧС и аварийных служб, врачи скорой помощи допускаются в Помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении ответственного лица Оператора.

3.7. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят у ответственного пользователя средств криптографической защиты информации.

3.8. При утрате ключа от хранилища или от входной двери в Помещение, замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает Оператор или ответственный пользователь средств криптографической защиты информации.

3.9. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в Помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю средств криптографической защиты информации или руководству Оператора. Прибывший ответственный пользователь средств криптографической защиты информации должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Положение
о порядке учета, хранения и уничтожения носителей персональных данных

I. Общие положения

1.1.Настоящее положение определяет порядок учета, хранения и уничтожения носителей персональных данных (далее – ПДн), регламентирует порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей ПДн и направлено на всех пользователей информационных систем (далее – ИС) Администрации городского округа Щёлково (далее – Оператор).

1.2.Настоящее положение разработано на основе Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3.ПДн субъектов хранятся на машинных и бумажных носителях.

1.4.Оператор обязан обеспечить учет всех защищаемых носителей информации с помощью их маркировки и занесения данных в Журнал учета машинных носителей информации, с отметкой об их выдаче (приеме).

1.5.Ответственность за организацию и осуществление учета, хранения и уничтожения носителей ПДн субъектов ПДн возлагается на администратора безопасности и администратора ИС.

1.6.Мероприятия по защите ПДн осуществляются администратором безопасности, администратором ИС или ответственным пользователем средств криптографической защиты в рамках выполнения своих обязанностей.

1.7.Условия хранения и обращения носителей ПДн должны исключать хищение, подмену и уничтожение носителей ПДн.

1.8.Оператор обязан обеспечить физическую защиту носителей ПДн, предусматривающую контроль доступа в помещения, в которых размещены элементы ИС, посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИС и хранилище носителей информации.

1.9. Уничтожение носителей информации осуществляется уполномоченной комиссией в строго регламентированном порядке. По результатам уничтожения носителей составляется соответствующий акт.

II. Организация работы с бумажными носителями персональных данных

2.1.Документ, содержащий ПДн, подлежит обязательному учету. Учет документов, содержащих ПДн, осуществляется в соответствии с установленными у Оператора правилами документооборота.

2.2.Для обеспечения физической сохранности бумажных носителей ПДн, предотвращения их хищения, а также для недопущения разглашения содержащихся в них сведений, документы должны храниться в сейфах, шкафах или тумбах, запираемых на ключ.

2.3.Хранение открытых документов вместе с конфиденциальными документами разрешено только в случаях, когда они являются приложениями к конфиденциальным документам.

2.4.Рабочее место сотрудников, обрабатывающих ПДн, должно быть организовано таким способом, чтобы была исключена возможность просмотра документов с ПДн, лицами, не допущенными к обработке ПДн.

2.5.На столе сотрудников, обрабатывающих ПДн, должны быть только те документы, с которыми ведется непосредственно работа, все остальные должны быть убраны в сейфы, тумбы или шкафы.

2.6.Все документы, содержащие ПДн, после окончания рабочего дня, должны убираться в запираемые сейфы, тумбы и шкафы. Перечень мест хранения носителей ПДн и сроки их хранения приведены в Правилах обработки персональных данных.

2.7.Ответственность за соблюдение норм, описанных в данном разделе, ложится на всех сотрудников, обрабатывающих ПДн.

2.8.Основанием для уничтожения документов является:

- достижение целей обработки;
- отзыв согласия субъекта на обработку его ПДн;
- получение соответствующего запроса от субъекта ПДн;
- получение соответствующего указания от уполномоченного органа по защите прав субъектов.

2.9.Уничтожение документов производится с помощью шредера, сжигания документов или ручным способом, путем разрыва документа на малые части или иными методами, принятыми у Оператора.

III. Организация работы с машинными носителями

3.1.Учету подлежат следующие типы машинных носителей ПДн:

- отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB-флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD, Blu-ray и прочее);
- неотчуждаемые носители информации (жесткие магнитные диски).

3.2.Все машинные носители ПДн, используемые при работе со средствами вычислительной техники (далее – СВТ) для обработки и хранения ПДн, обязательно регистрируются в Журнале учета машинных носителей информации.

3.3.Каждому машинному носителю, содержащему ПДн, присваивается учетный номер. За сотрудником, ответственным за СВТ, закрепляются установленные в данном СВТ несъемные жесткие магнитные диски.

3.4.Машинные носители ПДн выдаются пользователям или другим лицам, участвующим в обработке ПДн, для работы с соответствующей отметкой в Журнале учета машинных носителей информации.

3.5.После стирания ПДн машинные носители продолжают использоваться наравне с другими машинными носителями конфиденциальной информации. В последующем эти носители повторно используются для записи конфиденциальной информации.

3.6.В случае повреждения машинных носителей ПДн, работник, за которым закреплен носитель, сообщает о случившемся администратору безопасности.

3.7.Передача съемного машинного носителя ПДн третьим лицам производится в соответствии с требованиями договора между Оператором и третьим лицом.

3.8.При фиксации ПДн на машинных носителях не допускается фиксация на одном машинном носителе ПДн, цели обработки которых заведомо не совместимы.

3.9.Вынос машинных носителей ПДн за пределы контролируемой зоны Оператора запрещается без соответствующего разрешения руководства, если обратное не указано в регламенте работ сотрудника.

3.10.Хранение носителей, содержащих ПДн, осуществляется в условиях, исключающих возможность хищения, изменения целостности или уничтожения содержащейся на них информации.

3.11.Отчуждаемые носители ПДн после окончания работы с ними должны убираться в сейфы, тумбы или шкафы, запираемые на ключ.

3.12.Не допускается оставлять на рабочем столе или в СВТ машинные носители, содержащие ПДн.

3.13.Персональную ответственность за сохранность полученных машинных носителей и предотвращение несанкционированного доступа к записанным на них ПДн несет работник, за которым закреплен носитель.

3.14.Организация и осуществление правил хранения носителей резервного копирования производятся в соответствии с Порядком резервирования и восстановления работоспособности технических средств и программного обеспечения, защищаемой информации и средств защиты.

3.15.Под уничтожением носителя персональных данных понимаются действия, в результате которых становится невозможным восстановить материальный носитель ПДн.

3.16.Основанием для уничтожения машинных носителей ПДн является повреждение машинного носителя, исключающее его дальнейшее использование, или потеря практической ценности носителя.

3.17.Уничтожение носителей производится путем их физического разрушения с предварительным уничтожением содержащихся на них ПДн, если это позволяют физические принципы работы носителя.

3.18.Уничтожение машинных носителей производится комиссией. После уничтожения машинных носителей составляется Акт об уничтожении носителей персональных данных.

3.19.При уничтожении машинные носители данных снимаются с учета. Отметка об уничтожении машинных носителей проставляется в Журнале учета машинных носителей информации.

3.20.В случае допустимости повторного использования носителя информации применяется программное удаление («затирание») содержимого путем его форматирования с последующей записью новой информации на данный носитель.

3.21.Администратору безопасности при получении носителя должен обеспечить уничтожение записей или части записей с носителя и подготовить Акт об уничтожении персональных данных с машинного носителя. Подлежащие уничтожению файлы с ПДн, расположенные на жестком диске, удаляются средствами операционной системы компьютера с последующим «очищением корзины».

IV. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных

4.1.При подозрении или выявлении несоблюдения условий хранения носителей ПДн необходимо незамедлительно поставить в известность администратора безопасности или администратора ИС.

4.2.Разбирательство по факту несоблюдения условий хранения носителей ПДн информации назначается:

с момента подозрения на несоблюдение условий хранения носителей ПДн;

– с момента обнаружения несоблюдения условий хранения носителей ПДн.

– Для проведения разбирательства назначается комиссия в составе председателя комиссии и членов комиссии.

4.3.Комиссия в результате своей работы в течение семи дней должна установить:

– имела ли место утечка сведений конфиденциального характера и обстоятельства ей сопутствующие;

– установить лиц, виновных в нарушении несоблюдения условий хранения носителей ПДн;

– установить причину и условия, способствующие нарушению;

– выработать рекомендации по устранению установленных причин и условий и привести их в исполнение.

4.4.На время проведения разбирательства ПДн должны быть заблокированы.

4.5.По окончании разбирательства комиссия должна составить заключение по фактам несоблюдения условий хранения носителей ПДн.

4.6.В заключении указываются:

– обстоятельства, сопутствующие утечке сведений конфиденциального характера;

– лица, виновные в нарушении;

– причины и условия, способствующие нарушению;

– рекомендации по устранению установленных причин и условий.

V. Ответственность за нарушение порядка хранения и уничтожения персональных данных

5.1.Лица, виновные в нарушении порядка хранения и уничтожения персональных данных субъектов персональных данных, установленного действующим законодательством Российской Федерации и организационно-распорядительными документами Оператора, несут ответственность, предусмотренную законодательством Российской Федерации.

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

ФОРМА

АКТ № _____

уничтожения персональных данных с машинного носителя

Комиссия в соответствии с приказом от _____№ _____ в составе:

Председатель: _____ – _____
(ФИО) *(должность)*

Члены комиссии: _____ – _____
(ФИО) *(должность)*

_____ – _____
(ФИО) *(должность)*

составили настоящий акт в том, что произведено уничтожение персональных данных или иной конфиденциальной информации, находящейся на

_____
(наименование АРМ /заводской или учетный номер носителя информации)

Ответственный пользователь _____

_____
(ФИО, должность)

Уничтожения информации проведено путем _____

_____
(способ уничтожения)

Председатель: _____ _____
(ФИО) *(подпись)*

Члены комиссии: _____ _____
(ФИО) *(подпись)*

_____ _____
(ФИО) *(подпись)*

Акт составлен в _____ экз.

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

ФОРМА

АКТ № _____

уничтожения носителей персональных данных

Комиссия в соответствии с приказом от _____№ _____ в составе:

Председатель: _____ – _____
(ФИО) *(должность)*

Члены комиссии: _____ – _____
(ФИО) *(должность)*

_____ – _____
(ФИО) *(должность)*

составила настоящий акт о том, что произведено уничтожение носителей персональных данных в составе:

№ п/п	Дата	Тип носителя	Учетный номер носителя	Категория информации	Примечание

Всего подлежит уничтожению _____ носителей.
(цифрами и прописью количество)

На указанных носителях персональные данные уничтожены путем _____

_____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПДн уничтожены путем _____

_____
(разрезания/сжигания/размагничивания/физического уничтожения/механического уничтожения/иного способа)

Председатель: _____ _____
(ФИО) *(подпись)*

Члены комиссии: _____ _____
(ФИО) *(подпись)*

_____ _____
(ФИО) *(подпись)*

Акт составлен в _____ экз.

Утвержден распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

I. Перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн «Кадры», необходим для выполнения служебных обязанностей

№	ФИО сотрудника	Должность
1.	Алябьева Ольга Викторовна	Начальник отдела кадров и муниципальной службы
2.	Акимова Елена Валерьевна	Заместитель начальника отдела кадров и муниципальной службы
3.	Горчакова Ирина Анатольевна	Главный эксперт отдела кадров и муниципальной службы
4.	Гаврых Юлия Викторовна	Консультант отдела кадров и муниципальной службы
5.	Железцова Любовь Константиновна	Начальник сектора по профилактике коррупционных правонарушений отдела кадров и муниципальной службы
6.	Федотов Александр Александрович	Главный эксперт сектора по профилактике коррупционных правонарушений отдела кадров и муниципальной службы
7.	Попков Антон Сергеевич	Главный эксперт сектора по профилактике коррупционных правонарушений отдела кадров и муниципальной службы
8.	Новиков Алексей Иванович	Эксперт Административного управления
9.	Клешнев Игорь Борисович	Эксперт отдела организационной работы и информационной безопасности
10.	Халилуллин Руслан Ахмедович	Эксперт отдела организационной работы и информационной безопасности

II. Перечень лиц, имеющих право самостоятельного доступа в помещения, в которых производится обработка персональных данных ИСПДн «Кадры»

№	ФИО сотрудника	Должность
Кабинет № 101 (Серверная)		
1.	Новиков Алексей Иванович	Эксперт Административного управления
2.	Клешнев Игорь Борисович	Эксперт отдела организационной работы и информационной безопасности
3.	Халилуллин Руслан Ахмедович	Эксперт отдела организационной работы и информационной безопасности

Кабинет № 103		
1.	Новиков Алексей Иванович	Эксперт Административного управления
2.	Клешнев Игорь Борисович	Эксперт Отдела организационной работы и информационной безопасности
3.	Халилуллин Руслан Ахмедович	Эксперт Отдела организационной работы и информационной безопасности
Кабинет № 202		
1.	Акимова Елена Валерьевна	Заместитель начальника отдела кадров и муниципальной службы
2.	Попков Антон Сергеевич	Главный эксперт сектора по профилактике коррупционных правонарушений отдела кадров и муниципальной службы
3.	Клешнев Игорь Борисович	Эксперт отдела организационной работы и информационной безопасности
4.	Халилуллин Руслан Ахмедович	Эксперт отдела организационной работы и информационной безопасности
Кабинет № 203		
1.	Горчакова Ирина Анатольевна	Главный эксперт отдела кадров и муниципальной службы
2.	Гаврых Юлия Викторовна	Консультант отдела кадров и муниципальной службы
3.	Клешнев Игорь Борисович	Эксперт отдела организационной работы и информационной безопасности
4.	Халилуллин Руслан Ахмедович	Эксперт отдела организационной работы и информационной безопасности
Кабинет № 204		
1.	Алябьева Ольга Викторовна	Начальник отдела кадров и муниципальной службы
2.	Клешнев Игорь Борисович	Эксперт отдела организационной работы и информационной безопасности
3.	Халилуллин Руслан Ахмедович	Эксперт отдела организационной работы и информационной безопасности
Кабинет № 203		
1.	Железцова Любовь Константиновна	Начальник сектора по профилактике коррупционных правонарушений отдела кадров и муниципальной службы
2.	Федотов Александр Александрович	Главный эксперт сектора по профилактике коррупционных правонарушений отдела кадров и муниципальной службы
3.	Клешнев Игорь Борисович	Эксперт отдела организационной работы и информационной безопасности
4.	Халилуллин Руслан Ахмедович	Эксперт отдела организационной работы и информационной безопасности

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

ФОРМА
Лицевой счет пользователя
средств криптографической защиты информации
№____ от «__»_____20__г.

Данные о пользователе СКЗИ			
ФИО	Должность		
Данные о СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, числящихся за пользователем			
Наименование	Дата получения	Дата списания	Примечание

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Инструкция
пользователей в части обеспечения безопасности персональных данных при их обработке в информационных системах

I. Общие положения

1.1.Пользователь информационной системы (далее – Пользователь) осуществляет обработку персональных данных (далее – ПДн) в информационных системах (далее – ИС).

1.2.Пользователем является каждый сотрудник Администрации городского округа Щёлково (далее – Оператор), участвующий в рамках своих функциональных обязанностей в процессах обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3.Пользователь несет персональную ответственность за свои действия.

1.4.Пользователь в своей работе руководствуется настоящей инструкцией, Политикой в отношении обработки персональных данных, руководящими и нормативными документами ФСТЭК России, ФСБ России , а также регламентирующими документами Оператора.

1.5.Методическое руководство работой Пользователей осуществляется ответственным за организацию обработки персональных данных.

II. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих законодательных и нормативных правовых актов, а также внутренних инструкций, порядков, положений и других организационно-распорядительных документов, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Матрице разграничения доступа к ресурсам информационной системы.

2.3. Ознакомиться с прилагающимися к средствам защиты информации инструкциями.

2.4. Знать и соблюдать установленные требования по режиму обработки ПДн, учету, хранению и передаче носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.5. Соблюдать требования парольной политики.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получений консультаций по вопросам информационной безопасности, необходимо обращаться к администратору безопасности.

2.8. Для получения консультаций по вопросам работы и настройки элементов ИС необходимо обращаться к администратору ИС.

2.9. Своевременно информировать лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС.

2.10.Своевременно проходить обучение в области обработки и защиты ПДн. Проводить обучение, в пределах своих полномочий, имеют право: ответственный за организацию обработки персональных данных; администратор безопасности; администратор ИС, учреждение, специализирующееся на обучении лиц правилам работы с установленными средствами защиты информации; учреждение, производящее установку и настройку средств защиты информации.

2.11.После прохождения процедуры обучения, пользователь обязан знать цели применения средств защиты информации и порядок работы с ними. Пользователи, не усвоившие курс обучения, обязаны пройти его повторно до полного усвоения.

2.12.Пользователям запрещается:

- работать в ИС, пока они не усвоят порядок работы с установленными средствами защиты;
- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения администратора безопасности;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- подключать к рабочей станции и информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные правами доступа к ресурсам ИС;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИС;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с администратором безопасности.

2.13.При отсутствии визуального контроля над рабочей станцией, доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Заблокировать> (или нажать одновременно комбинацию клавиш <Win><L>).

2.14.Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий, в рамках возложенных на пользователя функций.

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 3410-р

Инструкция
по ведению журналов

I. Общие положения

1.1.Настоящая инструкция определяет порядок ведения журналов в Администрации городского округа Щёлково (далее – Оператор), а также лиц, ответственных за правильность и полноту ведения журналов.

1.2.Оператору для выполнения требований законодательства в области обеспечения безопасности персональных данных необходимо предусмотреть ведение следующих журналов:

- учета машинных носителей информации;
- учета мероприятий по контролю обеспечения защиты информации;
- учета обращений субъектов персональных данных о выполнении их законных прав, при обработке данных в информационных системах персональных данных;
- учета применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

1.3.Формы журналов утверждаются распоряжением Администрации городского округа Щёлково.

II. Ведение журнала учета машинных носителей информации

2.1 Машинные носители информации, используемые для обработки и хранения персональных данных Оператором, должны быть зарегистрированы в журнале учета машинных носителей информации.

2.2 Ведение Журнала осуществляется администратором безопасности совместно с администратором ИС.

2.3 У каждого носителя должен быть уникальный номер, которым является его заводской номер в соответствии с технической документацией, либо учетный номер, который может быть присвоен Оператором.

2.4 В качестве параметра Тип указывается тип носителя (HDD, DVD-RW, CD-R, USB-флеш-накопитель и т.д.).

2.5 В качестве параметра Емкость носителя указывается объем носителя в ГБ или МБ.

2.6 Все машинные носители должны выдаваться пользователям, несущим персональную ответственность за их сохранность под личную подпись с указанием даты в разделе Отметка о выдаче.

2.7 Неотчуждаемые носители информации (жесткие магнитные диски) закрепляются за сотрудником, ответственным за техническое средство, в котором установлен данный носитель, при этом при регистрации в графе Примечание указывается № аппаратных средств, с которыми осуществляется штатное функционирование.

2.8 При возврате носителя или технического средства, в котором установлен носитель, пользователь должен поставить подпись и дату возврата в разделе Отметка о возврате.

2.9 В журнале учета машинных носителей информации также должен отражаться факт уничтожения носителей, в случае уничтожения.

2.10 Отметка об уничтожении проставляется в графе Отметка об уничтожении с проставлением номера, даты акта уничтожения носителя и подписи ответственного.

III. Ведение журнала учета мероприятий по контролю обеспечения защиты информации

3.1.Журнал учета мероприятий по контролю обеспечения защиты информации (далее – Журнал) содержит перечень периодически проводимых мероприятий.

3.2.Ведение Журнала осуществляется лицами, участвующими в мероприятиях по защите информации: администратором безопасности, администратором ИС и ответственным пользователем средств криптографической защиты информации в рамках выполнения своих обязанностей.

3.3.Ответственный сотрудник ведет Журнал, вносит в него подробную информацию, связанную с изменением режима защиты персональных данных, информацию о результатах внутренних проверок выполнения режима защиты персональных данных, а также информацию о результатах периодических проверок средств защиты информации.

3.4.В Журнале указываются такие сведения, как: название проведенного мероприятия; дата проведения; исполнитель мероприятия (сотрудник Оператора или привлекаемая организация) и результат (отчет, акт, действия, при необходимости примечание).

IV. Ведение журнала обращений субъектов персональных данных о выполнении их законных прав, при обработке данных в информационных системах

4.1.Ответственным лицом за ведение журнала обращений субъектов персональных данных о выполнении их законных прав, при обработке данных в информационных системах (далее – Журнал) является ответственный за организацию обработки персональных данных. Сотрудники, участвующие в обработке запросов (в составлении ответов на запросы) могут вносить необходимые пометки в Журнал под контролем ответственного за организацию обработки персональных данных.

4.2.В Журнале указываются такие сведения, как: ФИО субъекта ПДн; дата обращения; регистрационный номер запроса, присваиваемый в соответствии с требованиями делопроизводства Оператора; цель обращения и результат.

4.3.Например, при получении запроса от субъекта в Журнал заносятся информация о субъекте, суть и цель запроса (информирование, уточнение, блокирование, удаление ПДн и т.д.). После обработки запроса перед отправкой ответа в Журнал (графа Результат) заносится окончательная информация: был составлен ответ или отказ, правовое обоснование ответа или отказа, дата, личная подпись лица, составлявшего ответ.

V. Ведение журнала учета применяемых средств защиты информации, эксплуатационной и технической документации к ним

5.1.Журнал учета применяемых средств защиты информации, эксплуатационной и технической документации к ним (далее – Журнал) содержит информацию о всех используемых или хранимым Оператором средств защиты информации и сопутствующей документации к ним.

5.2.Ведение Журнала осуществляется администратором безопасности.

5.3.В Журнале указываются наименования полученных средств защиты информации в соответствии с номенклатурой в сопроводительных документах, их регистрационные номера. В графе От кого получены указывается наименование организации, отгрузившей средства защиты информации, а в графе Дата и № сопроводительных документов указываются реквизиты договора/контракта/закрывающих бухгалтерских документов на поставку средств защиты информации (акт или товарная накладная).

5.4.При установке средств защиты информации в Журнале делается соответствующая запись с указанием ФИО, даты и подписи лица, непосредственно производившего установку.

5.5.Программные средства учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование (графа

№ аппаратных средств, в которые установлены или к которым подключены средства защиты).

5.6.Средства защиты информации могут изыматься из употребления. Отметка об изъятии проставляется в графе Примечание с проставлением номера, даты акта изъятии и подписи ответственного.

VI. Ведение журнала учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

6.1.Журнале учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал) содержит информацию о всех используемых или хранимых Оператором средств криптографической защиты информации и сопутствующей документации к ним.

6.2.Ведение Журнала осуществляется ответственным пользователем средств криптографической защиты информации.

6.3.В Журнале указываются наименования полученных средств криптографической защиты информации в соответствии с номенклатурой в сопроводительных документах, их регистрационные номера. В графе От кого получены указывается наименование организации, отгрузившей средства криптографической защиты информации, а в графе Дата и № сопроводительных документов указываются реквизиты договора/контракта/закрывающих бухгалтерских документов на поставку средств защиты информации (акт или товарная накладная).

6.4.Все экземпляры средств криптографической защиты, эксплуатационной и технической документации к ним должны выдаваться пользователям, несущим персональную ответственность за их сохранность под подпись в Журнале (раздел Отметка о выдаче).

6.5.При установке средств криптографической защиты информации в Журнале делается соответствующая запись с указанием ФИО, даты и подписи лица, непосредственно производившего установку.

6.6.Программные средства учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование (графа № аппаратных средств, в которые установлены или к которым подключены средства криптографической защиты).

6.7.По решению ответственного пользователя средств криптографической защиты информации средства криптографической защиты информации могут изыматься из употребления. Отметка об изъятии проставляется в разделе Отметка об изъятии СКЗИ, уничтожении ключевых документов с проставлением номера, даты акта об изъятии и подписи ответственного.

Утверждено распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Положение
по обработке персональных данных, осуществляемой без использования средств автоматизации

I. Общие положения

1.1. Настоящее положение разработано в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2. Обработка персональных данных (далее – ПДн), содержащихся в информационных системах (далее – ИС) Администрации городского округа Щёлково (далее – Оператор) либо извлеченных из таких систем, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с ПДн, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов ПДн, осуществляются при непосредственном участии человека.

1.3. Обработка ПДн не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что ПДн содержатся в ИС либо были извлечены из них.

1.4. Правила обработки ПДн, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Оператора, должны применяться с учетом требований настоящего Положения.

II. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

2.1 ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

2.2 При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

2.3 Лица, осуществляющие обработку ПДн без использования средств автоматизации, должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Оператора.

2.4 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки персональных данных, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки ПДн;

– типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку ПДн;

– 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;

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

2.5 При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же

носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

– при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

– при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

2.6 Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

2.7 Правила, предусмотренные пунктами 2.5 и 2.6 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе ПДн и информации, не являющейся ПДн.

2.8 Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального посителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

III. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

3.1. Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн, либо имеющих к ним доступ.

3.2. Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

3.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

Утверждена распоряжением
Администрации
городского округа Щёлково
от 12.12.2020 № 340-р

ФОРМА

Журнал учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Журнал начат: «____» _____ 20____ г.

Должность: _____

_____ /Ф. И. О. должностного лица/

Журнал окончен: «____» _____ 20____ г.

Должность: _____

_____ /Ф.И.О. должностного лица/

На _____листах

Щёлково 20__

№	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Регистрационный № СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов / номер экземпляра	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ, уничтожении ключевых документов			Примечание
			От кого получены	Дата и № сопроводительных документов	ФИО пользователя	Дата и подпись	ФИО лица, производившего подключение (установку)	Дата подключения и подпись	№ аппаратных средств, в которые установлены или к которым подключены СКЗИ	ФИО лица, производившего изъятие (уничтожение)	Дата изъятия (уничтожения)	Номер акта или расписка об уничтожении	
1.													
2.													
3.													
4.													
5.													
6.													
7.													
8.													
9.													

Утвержден распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Порядок
доступа в помещения, где осуществляется работа с персональными данными, и организация режима безопасности в этих помещениях

I. Общие положения

1. Настоящий порядок определяет:

– порядок доступа в помещения, где осуществляется обработка персональных данных (далее – ПДн) в информационных системах (далее – ИС);

– требования к организации режима безопасности в помещениях, где осуществляется работа с ПДн.

2. Настоящий документ распространяется на всех сотрудников Администрации городского округа Щёлково (далее – Оператор), имеющих право самостоятельного доступа в помещения, где ведется обработка ПДн.

3. Ответственность за режим безопасности помещений, где осуществляется обработка ПДн и где установлены средства защиты информации (далее – СЗИ), распространяется на всех сотрудников Оператора, имеющих право самостоятельного доступа в помещения, где ведется обработка ПДн.

4. Доступ в здание, где располагаются помещения, в которых обрабатываются ПДн, должен осуществляется в соответствии с режимом, исключающим возможность бесконтрольного входа (выхода) лиц и вноса (выноса) имущества.

5. Размещение, охрана и организация режима безопасности в помещениях, где установлены СЗИ и обрабатываются ПДн, должны обеспечивать сохранность ПДн субъектов персональных данных, СЗИ и ключевых документов к ним.

6. ПДн на материальных носителях должны находиться в недоступном для посторонних лиц месте.

7. При оборудовании помещений должны выполняться требования к размещению, монтажу СЗИ, а также другого устанавливаемого оборудования.

8. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

9. В нерабочее время помещения должны закрываться на ключ.

10. Размещение, специальное оборудование, охрана и организация режима безопасности в помещениях должны исключить возможность

неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

11. Установленный режим безопасности должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать требования настоящего Порядка.

12. Уборка помещений и все регламентные работы должны проводиться под контролем должностного лица, имеющего право самостоятельного доступа в помещения, согласно соответствующему Перечню лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных обязанностей, или иных ответственных лиц.

13. Все работы по обслуживанию технических средств проводятся только под контролем должностного лица, имеющего право самостоятельного доступа в помещения, согласно соответствующему Перечню лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных обязанностей, или иных ответственных лиц.

14. В рабочее время в помещениях обязательно должно присутствовать должностное лицо, имеющее право самостоятельного доступа в помещения, согласно соответствующему Перечню лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных обязанностей. При отсутствии такого лица вскрытие помещения и нахождение кого-либо в помещениях запрещается, и помещения должны закрываться на ключ.

15. При проведении закрытых мероприятий:

- двери и окна помещений должны быть закрыты;
- должна исключаться возможность утечки защищаемой информации по средствам телефонной связи.

16. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещение посторонних лиц, о случившемся должно быть немедленно сообщено руководству, а доступ в помещение должен быть ограничен.

17. В случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещение, в котором ведется обработка ПДн, вскрывается в сопровождении ответственного лица Оператора.

18. Повседневный контроль выполнения требований по защите помещений осуществляют должностные лица, имеющие право самостоятельного доступа в помещение, согласно соответствующему Перечню

лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных обязанностей.

19. При утрате ключа от входной двери в помещение, замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением.

20. Установка нового оборудования, мебели, и т.п. или замена их, а также ремонт помещений должны проводиться таким образом, чтобы была обеспечена конфиденциальность ПДн.

21. Размещение и монтаж другого оборудования, функционирующего в помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к элементам ИС. Техническое обслуживание такого оборудования осуществляется в присутствии лиц, имеющих право самостоятельного доступа в помещения.

Утвержден распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Перечень должностей служащих, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных

I. Основные положения

1.1. Настоящий перечень разработан в соответствии с требованиями Постановления Правительства Российской Федерации от 21 марта 2012 г. № 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».

1.2. В Администрации городского округа Щёлково ответственными должностями за проведение мероприятий по обезличиванию обрабатываемых персональных данных являются:

№	Отдел	Должность
1.	Отдел кадров и муниципальной службы	Начальник
		Заместитель начальника
		Главный эксперт
		Консультант
2.	Сектор по профилактике коррупционных правонарушений отдела кадров и муниципальной службы	Начальник
		Главный эксперт
3.	Административное управление	Эксперт
4.	Отдел организационной работы и информационной безопасности	Эксперт

Утвержден распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Перечень должностей служащих, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

I. Основные положения

1.1. Настоящий перечень разработан в соответствии с требованиями Постановления Правительства Российской Федерации от 21 марта 2012 г. № 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».

1.2. В Администрации городского округа Щёлково должностями, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным являются:

№	Отдел	Должность
1.	Отдел кадров и муниципальной службы	Начальник
		Заместитель начальника
		Главный эксперт
		Консультант
2.	Сектор по профилактике коррупционных правонарушений отдела кадров и муниципальной службы	Начальник
		Главный эксперт
3.	Административное управление	Эксперт
4.	Отдел организационной работы и информационной безопасности	Эксперт

Утвержден распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

I. Перечень лиц, допущенных к работе со средствами криптографической защиты информации

№	ФИО сотрудника	Должность
1.	Новиков Алексей Иванович	Эксперт Административного управления
2.	Клешнев Игорь Борисович	Эксперт отдела организационной работы и информационной безопасности
3.	Халилуллин Руслан Ахмедович	Эксперт отдела организационной работы и информационной безопасности
4.	Попков Антон Сергеевич	Главный эксперт сектора по профилактике коррупционных правонарушений отдела кадров и муниципальной службы
5.	Гаврых Юлия Викторовна	Консультант отдела кадров и муниципальной службы

II. Перечень лиц, имеющих право самостоятельного доступа в помещения, где осуществляется работа со средствами криптографической защиты информации

№	ФИО сотрудника	Должность
Кабинет № 101 (Серверная)		
1.	Новиков Алексей Иванович	Эксперт Административного управления
2.	Клешнев Игорь Борисович	Эксперт отдела организационной работы и информационной безопасности
3.	Халилуллин Руслан Ахмедович	Эксперт отдела организационной работы и информационной безопасности
Кабинет № 202		
1.	Акимова Елена Валерьевна	Заместитель начальника отдела кадров и муниципальной службы
2.	Попков Антон Сергеевич	Главный эксперт сектора по профилактике коррупционных правонарушений отдела кадров и муниципальной службы
3.	Клешнев Игорь Борисович	Эксперт отдела организационной работы и информационной безопасности
4.	Халилуллин Руслан Ахмедович	Эксперт отдела организационной работы и информационной безопасности
Кабинет № 203		
1.	Горчакова Ирина Анатольевна	Главный эксперт отдела кадров и муниципальной службы
2.	Гаврых Юлия Викторовна	Консультант отдела кадров и муниципальной службы
3.	Клешнев Игорь Борисович	Эксперт отдела организационной работы и информационной безопасности
4.	Халилуллин Руслан Ахмедович	Эксперт отдела организационной работы и информационной безопасности

Утвержден распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 310-р

План
мероприятий по защите информации в ИС

I. Общие положения

1. План мероприятий по защите информации в ИС (далее – План) разработан в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. План содержит необходимый перечень мероприятий для обеспечения безопасности информации и их периодичность.

3. Мероприятия по защите информации осуществляются, администратором безопасности, администратором ИС или ответственным пользователем средств криптографической защиты информации в рамках выполнения своих обязанностей.

4. По результатам проведения мероприятия ответственное должностное лицо осуществляет соответствующую запись в Журнале учета мероприятий по контролю обеспечения защиты информации[1].

5. Контроль выполнения мероприятий по обеспечению защиты информации осуществляется ответственным за организацию обработки персональных данных и/или руководством Администрации городского округа Щёлково (далее – Оператор).

План мероприятий по защите информации

№	Мероприятие	Периодичность	Исполнитель/ Ответственный
1.	Проверка наличия обновлений базы данных признаков вредоносных компьютерных программ и обновление при необходимости	Ежедневно	Администратор безопасности

[1] При настройке автоматического выполнения мероприятия и регистрации события в электронном журнале, запись в Журнале учета мероприятий по контролю обеспечения защиты информации

2.	Проверка работоспособности средства антивирусной защиты, обновления базы данных признаков вредоносных компьютерных программ	Ежемесячно	Администратор безопасности
3.	Проверка рабочих станций и работоспособности средств защиты информации	Ежеквартально / в случае возникновения инцидента	Администратор безопасности
4.	Проверка наличия документов, подтверждающих возможность применения средств защиты (сертификатов соответствия и других документов), обновление средств защиты информации при необходимости	Ежеквартально	Администратор безопасности
5.	Анализ журналов учета событий, регистрируемых средствами защиты	Ежемесячно / в случае возникновения инцидента	Администратор безопасности
6.	Смена паролей пользователей, проверка соблюдения требований парольной политики	Ежеквартально	Администратор ИС
7.	Заведение, удаление учетных записей пользователей; наделение, лишение, изменение полномочий пользователей по доступу к ресурсам информационных систем персональных данных	По мере необходимости (в случае изменений в структуре информационной системы персональных данных и (или) обработке информации, штатных изменений)	Администратор ИС
8.	Выявление, анализ и устранение уязвимостей ПО и сканирование сетевых портов	Ежеквартально	Администратор безопасности, администратор ИС
9	Обновление контента безопасности средства анализа защищенности	Перед проведением сканирования	Администратор безопасности
10.	Настройка и обновление программного обеспечения	При выпуске производителем критических обновлений и обновлений безопасности	Администратор ИС
11.	Резервное копирование данных	2 раза в месяц	Администратор ИС
12.	Резервное копирование эталонных копий ПО	Ежемесячно/ при внесении изменений в эталонные копии	Администратор ИС

13.	Проведение практических занятий и тренировок, мероприятий по обучению пользователей информационных систем персональных данных по вопросам обеспечения защиты информации	1 раз в 2 года (внепланово может проводиться по мере внесений изменений в Законодательство РФ, внедрении новых СЗИ, выявления новых угроз безопасности информации и т.д.)	Администратор безопасности, администратор ИС, ответственный за организацию обработки ПДн
14.	Актуализация/ доработка организационно-распорядительных документов, регламентирующих обработку и защиту информации	В случае изменений в структуре, составе информационной системы персональных данных и (или) обработке информации, штатных изменений, а также по мере внесений изменений в Законодательство РФ	Администратор безопасности, администратор ИС, ответственный за организацию обработки ПДн
15.	Ведение Журналов, необходимых для выполнения требований законодательства РФ в сфере обработки и защиты информации	По мере необходимости	Администратор безопасности, администратор ИС, ответственный пользователь средств криптографической защиты
16.	Контроль за соблюдением режима обработки ПДн	Раз в полгода (внепланово может проводиться при поступлении информации о нарушениях правил обработки ПДн)	Ответственный за организацию обработки ПДн
17.	Контроль выполнения мероприятий, предусмотренных планом мероприятий по защите информации	Ежегодно	Руководство Оператора, ответственный за организацию обработки ПДн
18.	Анализ изменения угроз безопасности информации в ИС и оценка возможных последствий их реализации	1 раз в 3 года (внепланово может проводиться в случае изменений в структуре ИС и (или) обработке информации)	Ответственный за организацию обработки ПДн
19.	Аттестация/переаттестация ИС	1 раз в 3 года	Организация-лицензиат ФСТЭК России

Утвержден распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Порядок
резервирования и восстановления работоспособности технических средств и программного обеспечения, защищаемой информации и средств защиты

I. Общие положения

1.1.Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, защищаемой информации и средств защиты информации определяет действия, связанные с функционированием информационных систем (далее - ИС) Администрации городского округа Щёлково (далее – Оператор), меры, и средства поддержания непрерывности работы и восстановления работоспособности ИС.

1.2.Целью настоящего документа является превентивная защита элементов ИС от потери защищаемой информации.

1.3.Задачей настоящего документа является определение действий по восстановлению в случае потери информации.

1.4.Действия настоящего документа распространяются на всех пользователей, имеющих доступ к ресурсам ИС, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- определение мер защиты от потери информации;
- системы контроля физического доступа.

1.5.Ответственность за выявление инцидентов и реагирование возлагается на администратора безопасности.

II. Порядок реагирования на инцидент

2.1.В настоящем документе под инцидентом понимается некоторое событие или группа событий, которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности информации (далее – инциденты).

2.2.Событие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИС;

– в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3.Все действия в процессе реагирования на инцидент должны документироваться администратором безопасности в Журнале учета мероприятий по контролю обеспечения защиты информации.

2.4.В ходе выявления инцидентов и реагирования на них осуществляются:

– обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– своевременное информирование пользователями ответственных лиц за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС;

– анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

2.5.В кратчайшие сроки, не превышающие одного рабочего дня, администратор безопасности предпринимает меры по восстановлению работоспособности ИС. Предпринимаемые меры по возможности согласуются с руководством. При необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

III. Технические меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1.К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

– системы жизнеобеспечения;

– системы обеспечения отказоустойчивости;

– системы контроля физического доступа.

Системы жизнеобеспечения включают:

– пожарные сигнализации и системы пожаротушения;

– системы резервного питания.

Системы обеспечения отказоустойчивости включают:

– кластеризация;

– технология RAID.

3.2.Помещения, в которых размещаются элементы ИС и средства защиты должны быть оборудованы средствами пожарной сигнализации.

3.3.Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны быть обеспечены бесперебойным снабжением электроэнергии. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

– локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

– источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

– дублированные системы электропитания в устройствах;

– резервные линии электропитания в пределах комплекса зданий;

– аварийные генераторы.

3.4.Для обеспечения отказоустойчивости критичных компонентов ИС при сбое в работе оборудования и их автоматической замены без простоев могут использоваться методы кластеризации. Для наиболее критичных компонентов ИС могут использоваться территориально удаленные системы кластеров.

3.5.Для защиты от отказов отдельных дисков автоматизированного рабочего места, осуществляющих обработку и хранение защищаемой информации, могут использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

IV. Организационные меры резервирования

4.1.Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на внешние носители (жесткий диск, оптический диск и т.п.).

4.2.Носители должны храниться в помещении, оборудованном системой пожаротушения.

4.3.Резервные копии должны храниться не менее года, для возможности их восстановления.

4.4.Резервное копирование и хранение данных должно осуществляться на периодической основе не реже двух раз в месяц.

4.5.Данные о проверке порядка резервного копирования должны отражаться в Журнале учета мероприятий по контролю обеспечения защиты информации.

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2008 № 340-р

ФОРМА

АКТ №_____

проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

«___» _____ 20___ года _____

_____

(должность, ФИО сотрудника/членов комиссии)

была проведена внутренняя проверка

_____

(тема проверки)

_____

В ходе проверки установлено: _____

_____

_____

Выявленные нарушения: _____

_____

_____

Меры по устранению нарушений: _____

_____

_____

Срок устранения нарушений: _____

_____

_____ _____ _____

(должность исполнителя) *(ФИО)* *(подпись)*

Утверждены распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

I. Общие положения

1.1. Настоящие правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152 ФЗ «О персональных данных», 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» и определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн), основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите ПДн.

II. Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

2.1. В целях осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн в Администрации городского округа Щёлково (далее – Оператор) проводятся периодические проверки условий обработки ПДн.

2.2. Проверка соответствия обработки ПДн требованиям к защите персональных данных осуществляется ответственным за организацию обработки персональных данных либо комиссией, состав которой утверждается соответствующим приказом.

2.3. Периодические проверки подразделяются на плановые и внеплановые.

2.4. Периодичность плановых проверок определяется в Плане мероприятий по защите информации в информационных системах.

2.5. Проведение внеплановой проверки организуется в течение трех рабочих дней со дня поступления информации о нарушениях правил обработки ПДн.

2.6. Проверка условий обработки ПДн осуществляются непосредственно на месте обработки ПДн путем опроса либо, при необходимости, путем осмотра служебных мест сотрудников, участвующих в процессе обработки ПДн.

2.7. При проведении проверки условий обработки ПДн должны быть полностью, объективно и всесторонне установлены:

– порядок и условия применения организационных и технических мер, необходимых для выполнения требований к защите ПДн;

– порядок и условия применения средств защиты информации;

– эффективность принимаемых мер по обеспечению безопасности ПДн;

– состояние учета носителей ПДн;

– соблюдение правил доступа к ПДн;

– соблюдение порядка доступа в помещения, в которых ведется обработка ПДн;

– наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер;

– мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.8. Ответственное лицо/комиссия за проведение проверки условий обработки ПДн имеет право:

– запрашивать у сотрудников Оператора информацию, необходимую для реализации полномочий;

– требовать от сотрудников Оператора, осуществляющих обработку ПДн, уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;

– выносить на рассмотрение руководства Оператора предложения о:

- совершенствовании правового, технического и организационного обеспечения безопасности ПДн при их обработке;
- приостановлении или прекращении обработки ПДн, осуществляемой с нарушением требований законодательства Российской Федерации;
- привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации о ПДн.

2.9. Лица, участвующие в проведении проверки условий обработки ПДн должны обеспечивать конфиденциальность ПДн, ставших им известными в ходе проведения мероприятий внутреннего контроля соответствия обработки ПДн.

2.10.Проверка условий обработки ПДн должна быть завершена не позднее чем через 30 календарных дней со дня принятия решения о ее проведении.

2.11.По результатам проведенной проверки условий обработки ПДн составляется Акт проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, в котором указываются: описание проведенных мероприятий; перечень и описание выявленных нарушений; рекомендации по устранению выявленных нарушений; заключение по итогам проведения внутреннего контроля.

2.12.Общая информация о проведенном контрольном мероприятии фиксируется в Журнале учета мероприятий по контролю обеспечения защиты информации.

Утверждены распоряжением
Администрации
городского округа Щёлково
от 19.12.2020 № 340-р

Правила
работы с обезличенными данными в случае обезличивания персональных данных

I. Общие положения

1.1. Настоящие Правила работы с обезличенными данными в случае обезличивания персональных данных (далее – Правила) разработаны в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных», Постановления 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».

1.2. Настоящие Правила регламентируют процесс обезличивания персональных данных (далее – ПДн) и работу с обезличенными данными в Администрации городского округа Щёлково (далее – Оператор).

1.3. Настоящие Правила обязательны для исполнения при работе с обезличенными данными.

II. Условия обезличивания ПДн

2.1. Обезличивание ПДн может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых ПДн, снижения уровня защищенности ПДн в информационных системах Оператора, в случае передачи носителей ПДн между пользователями, в сторонние организации для ремонта или утилизации и по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

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

2.3. Способы обезличивания при условии дальнейшей обработки ПДн:

– изменения перечня обрабатываемых сведений путем обобщения или удаления части сведений;

– замена части сведений идентификаторами с составлением таблицы соответствия идентификаторов исходным данным;

– понижение точности некоторых сведений путем перестановки части или групп сведений;

– деление сведений на части и последующая обработка в разных информационных системах.

2.4. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня обрабатываемых ПДн.

2.5. Для обезличивания ПДн приемлемы любые способы, явно не запрещенные законодательно.

2.6. К мероприятиям по обезличиванию обрабатываемых ПДн, допускаются лица, имеющие доступ к ПДн, в соответствии с перечнем должностей служащих, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных.

2.7. Решение о необходимости обезличивания ПДн принимается ответственным за организацию обработки персональных данных.

2.8. Способ обезличивания определяется ответственным за организацию обработки персональных данных.

2.9. Ответственный за организацию обработки персональных данных совместно с администратором безопасности, контролируют процесс обезличивания ПДн выбранным способом.

III. Правила работы с обезличенными данными

3.1. Обезличенные ПДн не подлежат разглашению и нарушению конфиденциальности.

3.2. Обезличенные ПДн могут обрабатываться с использованием и без использования средств автоматизации.

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

– парольной политики;

– антивирусной политики;

– правил работы со съемными носителями;

– правил резервного копирования;

– правил доступа в помещения, где расположены элементы информационных систем.

3.4. При обработке обезличенных ПДн без использования средств автоматизации необходимо соблюдение:

– правил хранения бумажных носителей;

– правил доступа к ним и в помещения, где они хранятся.

Утверждены распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Правила
обработки персональных данных

I. Общие положения

1.1. Настоящие Правила обработки персональных данных (далее – Правила) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют для каждой цели обработки персональных данных (далее – ПДн) содержание обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, сроки их обработки, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

1.2. Основные понятия, используемые в настоящих Правилах, соответствуют основным понятиям, установленным Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.3. Обработка ПДн в Администрации городского округа Щёлково (далее – Оператор) осуществляется как с использованием средств автоматизации, так и без использования средств автоматизации.

1.4. Глава городского округа Щёлково распоряжением назначает ответственного за организацию обработки персональных данных; утверждает комплект документации, регламентирующей обработку и защиту ПДн, а также осуществляет контроль за выполнением ответственными лицами и пользователями информационных систем своих обязанностей.

II. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

2.1. Для выявления и предотвращения нарушений законодательства Российской Федерации в сфере ПДн реализуются следующие процедуры:

– принятие мер, направленных на обеспечение выполнения Оператором своих обязанностей при обработке ПДн и прав субъекта ПДн;

– организация внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным действующим законодательством в области персональных данных, а также руководящими и регламентирующими документами Оператора;

– ознакомление сотрудников, осуществляющих обработку ПДн, с

законодательством Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, настоящими Правилами и (или) обучение сотрудников;

– ограничение обработки ПДн достижением конкретных, заранее определенных и законных целей;

– осуществление обработки ПДн в соответствии с принципами и условиями обработки ПДн, установленными законодательством Российской Федерации в области ПДн. Все субъекты ПДн должны предоставить согласие на обработку их ПДн Оператору, за исключением случаев, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– осуществление передачи ПДн только в случаях, предусмотренных федеральным законодательством и/или с согласия субъекта ПДн;

– недопущение обработки ПДн, несовместимых с целями их сбора и недопущение объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

– соответствие содержания и объема обрабатываемых ПДн заявленным целям обработки (обрабатываемые ПДн не избыточны по отношению к заявленным целям их обработки);

– обеспечение при обработке ПДн точности ПДн, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки ПДн.

III. Цели, содержание, сроки обработки и хранения персональных данных, обрабатываемых Оператором

№	Категории субъектов, ПДн которых обрабатываются	Цели обработки	Срок обработки / Условия прекращения обработки	Места хранения ПДн	Подразделения / должности, участвующие в обработке	Правовое основание обработки персональных данных
ИСПДн «Кадры»						
1.	Граждане, претендующие на замещение вакантных должностей	– осуществление подбора персонала	Срок обработки: до принятия решения о приеме / не приеме на работу и в течение 30 дней, в случае отказа в приеме на работу	Автоматизированные рабочие места, сервер, шкафы / стеллажи в кабинетах: № 101 (Серверная), № 103, № 202, № 203, № 204, № 205 расположенные по адресу: г. Щелково, пл. Ленина, д. 2	Отдел кадров и муниципальной службы: - начальник - заместитель начальника; - консультант; - главный эксперт Сектор по профилактике коррупционных правонарушений отдела кадров и муниципальной службы: - начальник; - главный эксперт Административное управление: - эксперт Отдел организационной работы и информационной безопасности: - эксперт	– Конституция РФ; – Трудовой кодекс РФ; – Гражданский кодекс РФ; – Согласие на обработку ПДн[1]
2.	Лица, включенные (претендующие на включение) в кадровый резерв	– формирование кадрового состава для замещения должностей муниципальной службы; – осуществление деятельности по профилактике коррупционных и иных правонарушений	Срок обработки: 3 года со дня завершения конкурса			– Конституция РФ; – Трудовой кодекс РФ; – Гражданский кодекс РФ; – Федеральный закон от 02 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации»; – Федеральный закон от 25 декабря 2008 года № 273-ФЗ «О противодействии коррупции»; – Согласие на обработку ПДн

[1] За исключением случаев, когда от имени соискателя действует кадровое агентство, а также при самостоятельном размещении соискателем своего резюме в сети Интернет

3.	Сотрудники (муниципальные служащие и лица, замещающие должности, не отнесенные к должностям муниципальной службы)	– организация кадрового делопроизводства Администрации; – подготовка и передача данных в контролирующие органы (ПФР, ФСС. ФНС, Росстат и прочие) в соответствии с требованиями законодательства, а также по запросу государственных органов; – осуществление деятельности по профилактике коррупционных и иных правонарушений	Срок обработки: – в течение срока действия и 3 года после окончания действия трудовых отношений[2]; – в течение срока действия и 10 лет после окончания действия трудового договора (контракта)[3] Условия прекращения обработки: перевод данных на архивное хранение	Автоматизированные рабочие места, сервер, шкафы / стеллажи в кабинетах: № 101 (Серверная), № 103, № 202, № 203, № 204, № 205 расположенные по адресу: г. Щелково, пл. Ленина, д. 2	Отдел кадров и муниципальной службы: - начальник - заместитель начальника; - консультант; - главный эксперт Сектор по профилактике коррупционных правонарушений отдела кадров и муниципальной службы: - начальник; - главный эксперт Административное управление: - эксперт Отдел организационной работы и информационной безопасности: - эксперт	– Конституция РФ; – Трудовой кодекс РФ; – Гражданский кодекс РФ; – Российской Федерации»; – Федеральный закон от 02 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации»; – Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»; – Трудовой договор (контракт); – Согласие на обработку ПДн
4.	Близкие родственники и члены семей сотрудников	– организация кадрового делопроизводства Администрации; – осуществление деятельности по профилактике коррупционных и иных правонарушений				– Конституция РФ; – Трудовой кодекс РФ; – Гражданский кодекс РФ; – Федеральный закон от 02 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации»; – Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»

[2] Сотрудники, замещающие должности, не относящиеся к должностям муниципальной службы

[3] Сотрудники, замещающие должности муниципальной службы

IV. Порядок хранения, использования и уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

4.1. ПДн субъектов хранятся на бумажных и электронных носителях.

4.2. Перечень ПДн закреплен в Перечне персональных данных, подлежащих защите в Администрации городского округа Щёлково.

4.3. Перечень лиц, доступ которых к ПДн субъектов необходим для выполнения служебных обязанностей, закреплен в соответствующих Перечнях лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных обязанностей.

4.4. Ответственным за организацию и осуществление хранения ПДн субъектов является ответственный за организацию обработки персональных данных, назначенный приказом руководства Оператора.

4.5. Ответственным за организацию и проведение мероприятий по обеспечению безопасности ПДн является ответственный за обеспечение безопасности персональных данных, назначенный приказом руководства Оператора.

4.6. Уничтожению подлежат ПДн при достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

4.7. Уничтожение ПДн может быть произведено любым способом, исключающим возможность восстановления ПДн.

4.8. Уничтожение бумажных носителей ПДн осуществляется соответствующей комиссией и фиксируется актом об уничтожении ПДн.

4.9. Уничтожение ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

V. Права субъектов в целях обеспечения защиты персональных данных, обрабатываемых Оператором

5.1. Субъекты имеют право получать полную информацию о своих ПДн.

5.2. Субъекты имеют право на получение информации, касающейся обработки их ПДн, в том числе содержащей: подтверждение факта обработки, правовые основания и цели обработки, способы и сроки обработки и т.д. в соответствии с законодательством РФ.

5.3. Субъекты имеют право бесплатного доступа к своим ПДн, включая право на получение копии любой записи, содержащей ПДн субъектов, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации возможно при личном обращении субъекта или его официального представителя.

5.4. Субъект имеет право требовать уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными.

5.5. Субъект имеет право требовать извещения Оператором всех лиц, которым ранее были сообщены его неверные или неполные ПДн, обо всех произведенных в них исключениях, исправлениях и дополнениях.

5.6. Субъект имеет право обжаловать в суде любые неправомерные действия или бездействия Оператора при обработке и защите его ПДн.

VI. Обязанности субъекта в целях обеспечения достоверности его персональных данных

6.1. До начала обработки ПДн субъект обязан представлять Оператору достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации.

6.2. При необходимости в случае изменения ПДн (смена паспорта, места жительства и т.д.) сообщать об этом Оператору.

VII. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн субъекта, установленных действующим законодательством Российской Федерации и организационно-распорядительными документами Оператора, несут ответственность, предусмотренную законодательством Российской Федерации.

VIII. Защита персональных данных

8.1. Для обеспечения защиты ПДн субъектов Оператором строится и вводится в действие система защиты. Построение системы защиты должно осуществляться на основании следующих документов:

1) Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2) Федеральный Закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.

3) Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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».

4) Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5) Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6) Нормативно-методические документы ФСТЭК России:

a. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

b. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15 февраля 2008 г. (ДСП);

c. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 14 февраля 2008 г;

7) Приказ Гостехкомиссии России от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;

8) Нормативно-методические документы ФСБ России:

a. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

b. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при

осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России № 149/7/2/6-432 от 31 марта 2015 г.

9) Частная(ые) модель(и) угроз.

10) Техническое(ие) задание(я).

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Матрица
разграничения доступа к ресурсам ИСПДн «Кадры»

№	Фамилия, имя, отчество (идентификатор)	Вид выполняемых функций	Защищаемые информационные ресурсы и установленные права доступа			
			Наименование ресурса	Место хранения ресурса	Права по доступу к ресурсу	Права по обработке ПДн
1.	Администратор безопасности: Клешнев И. Б. (Клешнев)	Администрирование средств защиты	Полный доступ к управлению и настройкам средств защиты информации, параметрам политики безопасности операционной системы, а также право просмотра персональных данных			
2.	Администратор ИС: Халилуллин Р. А. (Халилуллин)	Администрирование ИС	Полный доступ к настройкам ИС (за исключение управления и настройки средств защиты информации), а также право просмотра персональных данных			
3.	Операторы ИС: Гаврых Ю. В. (ГаврыхЮВ); Попков А. С. (ПопковАС).	Обработка информации (персональных данных)	Файлы ОС Windows	C:\Windows	RE	-
			Средство антивирусной защиты	C:\Program Files (x86)\Kaspersky Lab	RE	-
			Средство защиты информации от несанкционированного доступа	C:\DLLOCK80	RE	-
			Средство межсетевого экранирования	C:\DLLOCK80	RE	-
			Средство криптографической защиты информации	C:\Program Files\Crypto Pro	RE	-
			Средство обработки информации	C:\Program Files\PFR_RO-PD	RE	RWMD
			Средство обработки информации	C:\Program Files (x86)\Google	RE	RWMD
			Средство обработки информации	C:\Program Files (x86)\Microsoft Office	RE	RWMD
4.	Операторы ИС: Железцова Л. К. (ЖелезцоваЛК); Федотов А. А. (ФедотовАА); Алябьева О. В. (АлябьеваОВ); Горчакова И. А. (Горчакова); Акимова Е. В. (АкимоваЕВ).	Обработка информации (персональных данных)	Файлы ОС Windows	C:\Windows	RE	-
			Средство антивирусной защиты	C:\Program Files (x86)\Kaspersky Lab	RE	-
			Средство защиты информации от несанкционированного доступа	C:\DLLOCK80	RE	-
			Средство межсетевого экранирования	C:\DLLOCK80	RE	-
			Средство обработки информации	C:\Program Files\PFR_RO-PD	RE	RWMD
			Средство обработки информации	C:\Program Files (x86)\Google	RE	RWMD
			Средство обработки информации	C:\Program Files (x86)\Microsoft Office	RE	RWMD

R-чтение; W-запись; E-выполнение; M-изменение; D-удаление

Утверждено распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

ФОРМА
Типовое обязательство
сотрудника Администрации городского округа Щёлково о прекращении обработки персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, в случае увольнения или перехода на должность, не предусматривающую доступ к персональным данным

Я, _____
(фамилия, имя, отчество, должность)

_____

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае увольнения или перехода на должность, не предусматривающую доступ к персональным данным.

В соответствии со статьей 7 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Ответственность, предусмотренная Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснена.

_____ _____
(фамилия, инициалы) *(подпись)*

«__» _____ 20__ г.

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Политика
в отношении обработки персональных данных

I. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (п. 2 ст. 18.1) и излагает систему основных принципов, применяемых в отношении обработки персональных данных (далее – ПДн).

1.2. Администрация городского округа Щёлково является Оператором персональных данных (далее – Оператор, Администрация).

1.3. Политика подлежит изменению, дополнению в случае появления новых и изменения существующих законодательных актов и специальных нормативных документов об обработке и защите ПДн.

1.4. Политика распространяется на ПДн, полученные как до, так и после вступления в силу настоящей Политики.

1.5. Настоящая Политика определяет общие принципы, порядок и условия обработки ПДн физических лиц, чьи ПДн обрабатываются Оператором с целью обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн.

II. Ведение

2.1.Важным условием реализации целей деятельности Оператора является обеспечение необходимого и достаточного уровня информационной безопасности ПДн, обрабатываемых Оператором.

2.2.Оператор осуществляет обработку ПДн на законной и справедливой основе, в частности, в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2.3.Оператором разработаны и введены в действие документы, устанавливающие порядок обработки и защиты ПДн, которые обеспечивают соответствие требованиям Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятых в соответствии с ним локальных правовых актов и позволяют обеспечить защиту ПДн, обрабатываемых Оператором.

III. Персональные данные, обрабатываемые Оператором

3.1.Сведениями, составляющими ПДн, является любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту ПДн).

3.2.Состав ПДн определяется целями их обработки и фиксируется в Перечне персональных данных, подлежащих защите в Администрации городского округа Щёлково.

3.3.Оператор осуществляет обработку ПДн следующих типов субъектов:

1) *Граждан, претендующих на замещение вакантных должностей* со следующими целью: осуществление подбора персонала.

2) Лиц, включенных (претендующих на включение) в кадровый резерв со следующими целями:

– формирование кадрового состава для замещения должностей муниципальной службы;

– осуществление деятельности по профилактике коррупционных и иных правонарушений.

3) Сотрудников (муниципальных служащих и лиц, замещающих должности, не отнесенные к должностям муниципальной службы) со следующими целями:

– организация кадрового делопроизводства Администрации;

– подготовка и передача данных в контролирующие органы (ПФР, ФСС, ФНС, Росстат и прочие) в соответствии с требованиями законодательства, а также по запросу государственных органов;

– осуществление деятельности по профилактике коррупционных и иных правонарушений.

4) Близких родственников и членов семей сотрудников со следующими целями:

– организация кадрового делопроизводства Администрации;

– осуществление деятельности по профилактике коррупционных и иных правонарушений.

IV. Принципы и условия обработки персональных данных Оператором

4.1.Сроки обработки персональных данных определены в Правилах обработки персональных данных. Сроки обработки ПДн установлены в соответствии с требованиями законодательства Российской Федерации.

4.2.При обработке ПДн Оператором обеспечиваются их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн Оператором.

4.3.Оператор не осуществляет обработку специальных категорий ПДн.

4.4.Оператор не осуществляет обработку биометрических ПДн.

4.5.Оператор не осуществляет трансграничную передачу ПДн на территории иностранных государств.

4.6.ПДн обрабатываются Оператором как с помощью средств вычислительной техники, так и без использования таких средств и могут быть представлены как на бумажных, так и на электронных носителях. При этом Оператор выполняет все требования к автоматизированной и неавтоматизированной обработке ПДн, предусмотренные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним локальными правовыми актами, а также Постановлением Правительства от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4.7.Оператором не осуществляется принятие решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, на основании исключительно автоматизированной обработки ПДн.

4.8.Обработка ПДн Оператором осуществляется только с согласия субъектов ПДн за исключением следующих случаев:

– обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

– обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

– обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц.

4.9.Работники Оператора ознакомлены под личную подпись с документами, устанавливающими порядок обработки и защиты ПДн, а также права и обязанности, возникающие при осуществлении обработки и защиты ПДн.

4.10.ПДн поступают Оператору непосредственно от субъекта ПДн или от лиц, не являющихся субъектами ПДн. При этом Оператор выполняет все требования к осуществлению обработки таких данных, предусмотренные

Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», а также обеспечивает безопасность полученных ПДн.

4.11.Оператор осуществляет передачу ПДн третьим лицам на основании поручения обработки ПДн в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», в рамках исполнения норм действующего законодательства Российской Федерации, а также на основании согласия.

V.Права субъектов персональных данных, обрабатываемых Оператором

5.1.Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

– подтверждение факта обработки ПДн Оператором;

– правовые основания и цели обработки ПДн;

– цели и применяемые Оператором способы обработки ПДн;

– наименование и место нахождения Оператора, сведения о лицах (за исключением сотрудников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании федерального закона;

– обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки ПДн, в том числе сроки их хранения;

– порядок осуществления субъектом ПДн прав, предусмотренных федеральным законом;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные федеральными законами.

5.2.Субъект ПДн вправе потребовать у Оператора форму запроса информации, касающейся обработки ПДн субъекта. Для получения формы запроса субъекту необходимо обратиться по телефону _____ или по адресу электронной почты _____.

5.3.Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

5.4.Субъект ПДн вправе требовать от Оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются

необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.5.Сведения, касающиеся обработки ПДн субъекта, предоставляются ему Оператором в доступной форме, и не содержат ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

5.6.Сведения, касающиеся обработки ПДн субъекта, предоставляются ему или его представителю Оператором при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5.7.В случае если сведения, касающиеся обработки ПДн субъекта, а также если обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно к Оператору или направить повторный запрос не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

5.8.Субъект ПДн вправе обратиться повторно к Оператору или направить повторный запрос в целях получения сведений, касающихся обработки ПДн субъекта, а также в целях ознакомления с обрабатываемыми ПДн до истечения тридцати дней после первоначального обращения, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, касающимися обработки ПДн субъекта, должен содержать обоснование направления повторного запроса.

5.9.Если субъект ПДн считает, что Оператор осуществляет обработку его ПДн с нарушением требований федерального закона или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

5.10.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.

VI. Исполнение обязанностей Оператора персональных данных

6.1. Оператор исполняет обязанности, предусмотренные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним локальными правовыми актами, в том числе:

– сообщает субъекту ПДн или его представителю информацию, касающуюся обработки его ПДн, или предоставляет мотивированные отказы в предоставлении такой информации в форме и случаях и в сроки, предусмотренные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– разъясняет субъекту ПДн юридические последствия отказа предоставить его ПДн в предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» случаях;

– вносит необходимые изменения в ПДн, уничтожает их, уведомляет субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы, в срок и в случаях, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– уведомляет уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, в случае изменения сведений, касающихся обработки ПДн субъектов, а также в случае прекращения обработки ПДн в форме, в срок и случаях, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– сообщает в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в срок, предусмотренный Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– в случае достижения цели обработки ПДн обеспечивает прекращение обработки ПДн и их уничтожение в срок, предусмотренный Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

6.2. Оператором для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним локальными правовыми актами, приняты следующие необходимые и достаточные меры:

– назначен ответственный за организацию обработки персональных данных;

– приняты локальные правовые акты по вопросам обработки и защиты ПДн, а также локальные правовые акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

– применены правовые, организационные и технические меры по обеспечению безопасности ПДн;

– осуществляется внутренний контроль соответствия обработки ПДн требованиям Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятых в соответствии с ним локальных правовых актов, настоящей Политики;

– проведена оценка вреда, который может быть причинен субъектам ПДн в случае нарушения требований федерального законодательства о ПДн, произведено соотношение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятых в соответствии с ним локальных правовых актов;

– сотрудники Оператора, непосредственно осуществляющие обработку ПДн, ознакомлены с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятых в соответствии с ним локальных правовых актов, настоящей Политики и локальных правовых актов по вопросам обработки ПДн.

VII. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

7.1.Лица, виновные в нарушении требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» во исполнение которого разработана настоящая Политика, несут гражданско-правовую, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

VIII. Изменение Политики

8.1.Оператор имеет право вносить изменения в настоящую Политику.

8.2.При внесении изменений в заголовке Политики указывается дата последнего обновления редакции.

8.3.При внесении изменений новая редакция Политики утверждается приказом.

8.4.Новая редакция Политики вступает в силу с даты утверждения соответствующего приказа, если иное не предусмотрено приказом.

Утвержден распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Регламент
технологического процесса обработки защищаемой информации в ИСПДн «Кадры»

I. Общие положения

1.1. Настоящий регламент определяет процесс обработки персональных данных (далее – ПДн) в информационной системе персональных данных (далее – ИСПДн) «Кадры», а также процесс обеспечения защиты информации при выводе из эксплуатации данной информационной системы или после принятия решения об окончании обработки информации в ИСПДн «Кадры».

1.2. Настоящий регламент разработан в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Доступ к ИСПДн «Кадры» должен быть ограничен в соответствии с Перечнем лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн «Кадры», необходим для выполнения служебных обязанностей.

1.4. Обработке должны подлежать только ПДн, указанные в Перечне персональных данных, подлежащих защите в Администрации городского округа Щёлково.

1.5. При доступе к ПДн необходимо использовать объекты доступа, указанные в Техническом паспорте ИСПДн «Кадры».

1.6. Обработка ПДн должна осуществляться в защищаемых помещениях в соответствии с Техническим паспортом ИСПДн «Кадры».

1.7. Доступ пользователей к ПДн должен осуществляться под своей учетной записью и в соответствии с Матрицей разграничения доступа к ресурсам ИСПДн «Кадры».

1.8. Основными целями функционирования ИСПДн «Кадры» и обработки персональных данных в ней являются:

– осуществление подбора персонала;

– формирование кадрового состава для замещения должностей муниципальной службы;

– организация кадрового делопроизводства Администрации;

– подготовка и передача данных в контролирующие органы (ПФР, ФСС, ФНС, Росстат и прочие) в соответствии с требованиями законодательства, а также по запросу государственных органов;

– осуществление деятельности по профилактике коррупционных и иных правонарушений.

1.9. Доступ к ПДн должен осуществляться через программный продукт «1С:Предприятие», браузер Google Chrome посредством подключения к Порталу mosreg.ru, через офисный пакет Microsoft Office, а также посредством физического доступа к носителям ПДн.

1.10.Высшим грифом конфиденциальности обрабатываемой информации в ИСПДн «Кадры» может быть гриф «Для служебного пользования».

1.11.Для защиты информации в ИСПДн «Кадры» необходимо использовать следующие средства защиты:

– средства управления и разграничения доступа пользователей;

– средства антивирусной защиты;

– средства защиты от несанкционированного доступа;

– средства межсетевого экранирования;

– средства защиты каналов связи;

– средства криптографической защиты;

– средства анализа защищенности.

1.12.В случае выявления инцидентов при обработке ПДн в ИСПДн «Кадры» ответственными лицами должны быть приняты все необходимые меры в соответствии с инструкциями и положениями, утвержденными Оператором (Оператор – Администрация городского округа Щёлково).

1.13.Контроль (мониторинг) за обеспечением уровня защищенности ПДн в ИСПДн «Кадры» осуществляется ответственными за данный контроль лицами, в пределах их полномочий.

1.14.В случае принятия решения об окончании обработки ПДн и при выводе из эксплуатации ИСПДн «Кадры» необходимо предпринимать меры, направленные на обеспечение защиты ПДн на срок, предусмотренный федеральным законодательством. Предпринимаемые меры могут включать в себя:

– архивирование информации, содержащейся в ИСПДн «Кадры» (осуществляется при необходимости дальнейшего использования информации в деятельности Оператора);

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации (производится при необходимости передачи машинного носителя информации другому пользователю ИСПДн «Кадры» или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения);

– уничтожение машинных носителей информации (производится при выводе машинных носителей из эксплуатации).

Утвержден распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Перечень
персональных данных, подлежащих защите в Администрации городского округа Щёлково

I. Основные положения

1.1. Настоящий перечень разработан в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления 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».

1.2. В соответствии с Перечнем систем Администрации городского округа Щёлково, осуществляется обработка персональных данных (далее – ПДн) в следующих информационных системах.

II. Информационная система персональных данных «Кадры» (ИСПДн «Кадры»)

Основными целями функционирования ИСПДн «Кадры» и обработки персональных данных в ней являются:

- осуществление подбора персонала;
- формирование кадрового состава для замещения должностей муниципальной службы;
- организация кадрового делопроизводства Администрации;
- подготовка и передача данных в контролирующие органы (ПФР, ФСС, ФНС, Росстат и прочие) в соответствии с требованиями законодательства, а также по запросу государственных органов;
- осуществление деятельности по профилактике коррупционных и иных правонарушений.

2.1.Описание типов субъектов персональных данных

В ИСПДн «Кадры» обрабатываются персональные данные следующих субъектов:

- граждане, претендующие на замещение вакантных должностей;
- лица, включенные (претендующие на включение) в кадровый резерв;

- сотрудники (муниципальные служащие и лица, замещающие должности, не отнесенные к должностям муниципальной службы);
- близкие родственники и члены семей сотрудников.

2.2. Состав сведений, составляющих персональные данные

В ИСПДн «Кадры» обрабатываются следующие персональные данные:

1) Персональные данные граждан, претендующих на замещение вакантных должностей:

- фамилия, имя, отчество (если изменялись ФИО, то указывается, когда, где и по какой причине);
- число, месяц, год рождения;
- место рождения;
- сведения о гражданстве (в том числе в случае изменения гражданства – предыдущие гражданства, иные гражданства, дата и причина изменения гражданства);
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- адрес места жительства (адрес регистрации, фактического проживания);
- номер контактного телефона или сведения о других способах связи;
- реквизиты страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- фотография[1];
- сведения о служебной (трудовой) деятельности;
- сведения о воинском учете и реквизиты документов воинского учета;
- сведения об образовании (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, направление подготовки или специальность, квалификация по документу об образовании);
- сведения о послевузовском профессиональном образовании (наименование и год окончания образовательной или научной организации), ученой степени, ученом звании (дата присвоения, номера дипломов, аттестатов);
- сведения о владении иностранными языками, степень владения;
- сведения о наличии или отсутствии судимости;
- сведения об оформленных допусках к государственной тайне (форма, номер и дата);

[1] Не используется для идентификации субъекта

– государственные награды, иные награды и знаки отличия (кем и когда награжден);

– сведения о профессиональной переподготовке и (или) повышении квалификации

– иные персональные данные, предоставленные субъектом.

2) Персональные данные лиц, включенных (претендующих на включение) в кадровый резерв:

– фамилия, имя, отчество (если изменялись ФИО, то указывается, когда, где и по какой причине);

– число, месяц, год рождения;

– место рождения;

– сведения о гражданстве (в том числе в случае изменения гражданства – предыдущие гражданства, иные гражданства, дата и причина изменения гражданства);

– вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

– адрес места жительства (адрес регистрации, фактического проживания);

– номер контактного телефона или сведения о других способах связи;

– реквизиты страхового свидетельства государственного пенсионного страхования;

– идентификационный номер налогоплательщика;

– реквизиты страхового медицинского полиса обязательного медицинского страхования;

– реквизиты свидетельства государственной регистрации актов гражданского состояния;

– фотография[2];

– семейное положение, состав семьи и сведения о близких родственниках (отце, матери, братьях, сестрах и детях), а также о муже (жене);

– сведения о служебной (трудовой) деятельности;

– сведения о воинском учете и реквизиты документов воинского учета;

– сведения об образовании (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, направление подготовки или специальность, квалификация по документу об образовании);

[2] Не используется для идентификации субъекта

– сведения о послевузовском профессиональном образовании (наименование и год окончания образовательной или научной организации), ученой степени, ученом звании (дата присвоения, номера дипломов, аттестатов);

– сведения о владении иностранными языками, степень владения;

– результаты обязательных предварительных (при поступлении на муниципальную службу, работу, участии в конкурсе на включение в кадровый резерв) и периодических медицинских осмотров;

– сведения о пребывании за границей (страна, год и цель пребывания), серия номер заграничного паспорта, наименование органа, выдавшего его, дата выдачи;

– сведения о присвоенном классном чине федеральной муниципальной службы, муниципальной службы субъекта Российской Федерации, муниципальной службы, дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы (кем и когда присвоен);

– сведения о наличии или отсутствии судимости;

– сведения об оформленных допусках к государственной тайне (форма, номер и дата);

– государственные награды, иные награды и знаки отличия (кем и когда награжден);

– сведения о профессиональной переподготовке и (или) повышении квалификации

– сведения о доходах, об имуществе и обязательствах имущественного характера;

– номер расчетного счета;

– номер банковской карты;

– занимаемая должность;

– иные персональные данные, предоставленные субъектом.

3) Персональные данные сотрудников (муниципальных служащих и лиц, замещающих должности, не отнесенные к должностям муниципальной службы):

– фамилия, имя, отчество (если изменялись ФИО, то указывается, когда, где и по какой причине);

– число, месяц, год рождения;

– место рождения;

– сведения о гражданстве (в том числе в случае изменения гражданства – предыдущие гражданства, иные гражданства, дата и причина изменения гражданства);

– вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

– адрес места жительства (адрес регистрации, фактического проживания);

– номер контактного телефона или сведения о других способах связи;

– реквизиты страхового свидетельства государственного пенсионного страхования;

– идентификационный номер налогоплательщика;

– реквизиты страхового медицинского полиса обязательного медицинского страхования;

– реквизиты свидетельства государственной регистрации актов гражданского состояния;

– фотография[3];

– семейное положение, состав семьи и сведения о близких родственниках (отце, матери, братьях, сестрах и детях), а также о муже (жене);

– сведения о служебной (трудовой) деятельности;

– данные о трудовом договоре (контракте) (№ трудового договора (контракта), дата его заключения, дата начала и дата окончания договора (контракта), вид работы, срок действия договора (контракта), наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору (контракту), характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);

– сведения о приеме на работу, перемещении по должности, увольнении;

– сведения об отпусках;

– сведения о командировках;

– сведения о временной нетрудоспособности[4];

– сведения о воинском учете и реквизиты документов воинского учета;

– сведения об образовании (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, направление подготовки или специальность, квалификация по документу об образовании);

[3] Не используется для идентификации субъекта

[4] В электронном виде обрабатывается только продолжительность больничного

– сведения о послевузовском профессиональном образовании (наименование и год окончания образовательной или научной организации), ученой степени, ученом звании (дата присвоения, номера дипломов, аттестатов);

– сведения о владении иностранными языками, степень владения;

– результаты обязательных предварительных (при поступлении на муниципальную службу, работу, участии в конкурсе на включение в кадровый резерв) и периодических медицинских осмотров;

– сведения о пребывании за границей (страна, год и цель пребывания), серия номер заграничного паспорта, наименование органа, выдавшего его, дата выдачи;

– сведения о присвоенном классном чине федеральной муниципальной службы, муниципальной службы субъекта Российской Федерации, муниципальной службы, дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы (кем и когда присвоен);

– сведения о наличии или отсутствии судимости;

– сведения об оформленных допусках к государственной тайне (форма, номер и дата);

– государственные награды, иные награды и знаки отличия (кем и когда награжден);

– сведения о профессиональной переподготовке и (или) повышении квалификации

– сведения о доходах, об имуществе и обязательствах имущественного характера;

– номер расчетного счета;

– номер банковской карты;

– занимаемая должность;

– иные персональные данные, предоставленные субъектом.

4) Персональные данные близких родственников и членов семей сотрудников:

– фамилия, имя, отчество;

– число, месяц, год и место рождения;

– адрес регистрации по месту жительства или по месту пребывания, адрес фактического проживания;

– степень родства;

– сведения о доходах, об имуществе и обязательствах имущественного характера.

Утверждено распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Форма согласия на обработку персональных данных

I. Согласие
на обработку персональных данных для граждан, претендующих на замещение вакантных должностей

Я, _____,
(ФИО)

паспорт _____ выдан _____ ___,
(серия, номер) *(когда и кем выдан)*

Адрес регистрации: _____,

в соответствии с Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных» даю согласие Администрации городского округа Щёлково (далее - Оператор) ОГРН 1035010204745, ИНН 5050002154, зарегистрированной по адресу: Московская область, г. Щёлково, пл. Ленина, д. 2, на обработку моих персональных данных с целью осуществления подбора персонала.

Обработка включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Перечень персональных данных, на обработку которых даю согласие:

- фамилия, имя, отчество (если изменялись ФИО, то указывается, когда, где и по какой причине);
- число, месяц, год рождения;
- место рождения;
- сведения о гражданстве (в том числе в случае изменения гражданства – предыдущие гражданства, иные гражданства, дата и причина изменения гражданства);
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- адрес места жительства (адрес регистрации, фактического проживания);
- номер контактного телефона или сведения о других способах связи;
- реквизиты страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- фотография[1];
- сведения о служебной (трудовой) деятельности;
- сведения о воинском учете и реквизиты документов воинского учета;
- сведения об образовании (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, направление подготовки или специальность, квалификация по документу об образовании);
- сведения о послевузовском профессиональном образовании (наименование и год окончания образовательной или научной организации), ученой степени, ученом звании (дата присвоения, номера дипломов, аттестатов);
- сведения о владении иностранными языками, степень владения;
- сведения о наличии или отсутствии судимости;
- сведения об оформленных допусках к государственной тайне (форма, номер и дата);
- государственные награды, иные награды и знаки отличия (кем и когда награжден);
- сведения о профессиональной переподготовке и (или) повышении квалификации
- иные персональные данные, предоставленные субъектом.

С персональными данными может производиться автоматизированная и неавтоматизированная обработка.

Согласие действует с момента подписания и до принятия решения о приеме/не приеме на работу и в течение 30 дней, в случае отказа в приеме на работу

Действие настоящего Согласия прекращается досрочно в случае принятия Оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

«____» _____ 20____ г. _____
(подпись)

[1] Не используется для идентификации субъекта

II. Согласие
на обработку персональных данных для лиц, включенных (претендующих на включение) в кадровый резерв

Я, _____,
(ФИО)

паспорт _____ выдан _____,
(серия, номер) *(когда и кем выдан)*

Адрес регистрации: _____,

в соответствии с Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных» даю согласие Администрации городского округа Щёлково (далее - Оператор) ОГРН 1035010204745, ИНН 5050002154, зарегистрированной по адресу: Московская область, г. Щёлково, пл. Ленина, д. 2, на обработку моих персональных данных в целях:

- формирование кадрового состава для замещения должностей муниципальной службы;
- осуществление деятельности по профилактике коррупционных и иных правонарушений.

Обработка включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Перечень персональных данных, на обработку которых даю согласие:

- фамилия, имя, отчество (если изменялись ФИО, то указывается, когда, где и по какой причине);
- число, месяц, год рождения;
- место рождения;
- сведения о гражданстве (в том числе в случае изменения гражданства – предыдущие гражданства, иные гражданства, дата и причина изменения гражданства);
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- адрес места жительства (адрес регистрации, фактического проживания);
- номер контактного телефона или сведения о других способах связи;
- реквизиты страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- реквизиты страхового медицинского полиса обязательного медицинского страхования;
- реквизиты свидетельства государственной регистрации актов гражданского состояния;
- фотография[2];
- семейное положение, состав семьи и сведения о близких родственниках (отце, матери, братьях, сестрах и детях), а также о муже (жене);
- сведения о служебной (трудовой) деятельности;
- сведения о воинском учете и реквизиты документов воинского учета;
- сведения об образовании (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, направление подготовки или специальность, квалификация по документу об образовании);
- сведения о послевузовском профессиональном образовании (наименование и год окончания образовательной или научной организации), ученой степени, ученом звании (дата присвоения, номера дипломов, аттестатов);
- сведения о владении иностранными языками, степень владения;
- результаты обязательных предварительных (при поступлении на муниципальную службу, работу, участии в конкурсе на включение в кадровый резерв) и периодических медицинских осмотров;
- сведения о пребывании за границей (страна, год и цель пребывания), серия номер заграничного паспорта, наименование органа, выдавшего его, дата выдачи;
- сведения о присвоенном классном чине федеральной муниципальной службы, муниципальной службы субъекта Российской Федерации, муниципальной службы, дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы (кем и когда присвоен);
- сведения о наличии или отсутствии судимости;
- сведения об оформленных допусках к государственной тайне (форма, номер и дата);
- государственные награды, иные награды и знаки отличия (кем и когда награжден);
- сведения о профессиональной переподготовке и (или) повышении квалификации
- сведения о доходах, об имуществе и обязательствах имущественного характера;
- номер расчетного счета;
- номер банковской карты;

[2] Не используется для идентификации субъекта

– занимаемая должность;
– иные персональные данные, предоставленные субъектом.

С персональными данными может производиться автоматизированная и неавтоматизированная обработка.

Согласие действует с момента подписания и в течении трех лет со дня завершения конкурса

Действие настоящего Согласия прекращается досрочно в случае принятия Оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

«____» _____ 20____ г. _____
(подпись)

III. Согласие на обработку персональных данных для сотрудников (муниципальных служащих)

Я, _____,
(ФИО)

паспорт _____ выдан _____,
(серия, номер) *(когда и кем выдан)*

Адрес регистрации: _____,

в соответствии с Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных» даю согласие Администрации городского округа Щёлково (далее - Оператор) ОГРН 1035010204745, ИНН 5050002154, зарегистрированной по адресу: Московская область, г. Щёлково, пл. Ленина, д. 2, на обработку моих персональных данных в целях:

– организация кадрового делопроизводства Администрации;
– подготовка и передача данных в контролирующие органы (ПФР, ФСС, ФНС, Росстат и прочие) в соответствии с требованиями законодательства, а также по запросу государственных органов;
– осуществление деятельности по профилактике коррупционных и иных правонарушений.

Обработка включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Перечень персональных данных, на обработку которых даю согласие:

– фамилия, имя, отчество (если изменялись ФИО, то указывается, когда, где и по какой причине);
– число, месяц, год рождения;
– место рождения;
– сведения о гражданстве (в том числе в случае изменения гражданства – предыдущие гражданства, иные гражданства, дата и причина изменения гражданства);
– вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
– адрес места жительства (адрес регистрации, фактического проживания);
– номер контактного телефона или сведения о других способах связи;
– реквизиты страхового свидетельства государственного пенсионного страхования;
– идентификационный номер налогоплательщика;
– реквизиты страхового медицинского полиса обязательного медицинского страхования;
– реквизиты свидетельства государственной регистрации актов гражданского состояния;
– фотография[3];
– семейное положение, состав семьи и сведения о близких родственниках (отце, матери, братьях, сестрах и детях), а также о муже (жене);
– сведения о служебной (трудовой) деятельности;

[3] Не используется для идентификации субъекта

– данные о трудовом договоре (контракте) (№ трудового договора (контракта), дата его заключения, дата начала и дата окончания договора (контракта), вид работы, срок действия договора (контракта), наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору (контракту), характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
– сведения о приеме на работу, перемещении по должности, увольнении;
– сведения об отпусках;
– сведения о командировках;
– сведения о временной нетрудоспособности[4];
– сведения о воинском учете и реквизиты документов воинского учета;
– сведения об образовании (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, направление подготовки или специальность, квалификация по документу об образовании);
– сведения о послевузовском профессиональном образовании (наименование и год окончания образовательной или научной организации), ученой степени, ученом звании (дата присвоения, номера дипломов, аттестатов);
– сведения о владении иностранными языками, степень владения;
– результаты обязательных предварительных (при поступлении на муниципальную службу, работу, участии в конкурсе на включение в кадровый резерв) и периодических медицинских осмотров;
– сведения о пребывании за границей (страна, год и цель пребывания), серия номер заграничного паспорта, наименование органа, выдавшего его, дата выдачи;
– сведения о присвоенном классном чине федеральной муниципальной службы, муниципальной службы субъекта Российской Федерации, муниципальной службы, дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы (кем и когда присвоен);
– сведения о наличии или отсутствии судимости;
– сведения об оформленных допусках к государственной тайне (форма, номер и дата);
– государственные награды, иные награды и знаки отличия (кем и когда награжден);
– сведения о профессиональной переподготовке и (или) повышении квалификации
– сведения о доходах, об имуществе и обязательствах имущественного характера;
– номер расчетного счета;
– номер банковской карты;
– занимаемая должность;
– иные персональные данные, предоставленные субъектом.

С персональными данными может производиться автоматизированная и неавтоматизированная обработка.

Также я даю/не даю (нужное подчеркнуть) согласие на включение в общедоступные источники информации такие как официальный сайт Администрации городского округа Щёлково с целью предоставления контактных сведений и информации о структуре посетителям официального сайта, следующих моих персональных данных: фамилия, имя, отчество, должность, номер телефона (нужное подчеркнуть).

Согласие действует в течение действия трудовых отношений и 10 лет после их окончания.

Действие настоящего Согласия прекращается досрочно в случае принятия Оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

«____» _____ 20____ г. _____
(подпись)

[4] В электронном виде обрабатывается только продолжительность больничного

IV. Согласие
на обработку персональных данных для сотрудников (лиц, замещающих должности, не отнесенные к должностям муниципальной службы)

Я, _____,
(ФИО)

паспорт _____ выдан _____,
(серия, номер) *(когда и кем выдан)*

Адрес регистрации: _____,

в соответствии с Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных» даю согласие Администрации городского округа Щёлково (далее - Оператор) ОГРН 1035010204745, ИНН 5050002154, зарегистрированной по адресу: Московская область, г. Щёлково, пл. Ленина, д. 2, на обработку моих персональных данных в целях:

– организация кадрового делопроизводства Администрации;

– подготовка и передача данных в контролирующие органы (ПФР, ФСС, ФНС, Росстат и прочие) в соответствии с требованиями законодательства, а также по запросу государственных органов.

Обработка включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Перечень персональных данных, на обработку которых даю согласие:

– фамилия, имя, отчество (если изменялись ФИО, то указывается, когда, где и по какой причине);

– число, месяц, год рождения;

– место рождения;

– сведения о гражданстве (в том числе в случае изменения гражданства – предыдущие гражданства, иные гражданства, дата и причина изменения гражданства);

– вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

– адрес места жительства (адрес регистрации, фактического проживания);

– номер контактного телефона или сведения о других способах связи;

– реквизиты страхового свидетельства государственного пенсионного страхования;

– идентификационный номер налогоплательщика;

– реквизиты страхового медицинского полиса обязательного медицинского страхования;

– реквизиты свидетельства государственной регистрации актов гражданского состояния;

– фотография[5];

– семейное положение, состав семьи и сведения о близких родственниках (отце, матери, братьях, сестрах и детях), а также о муже (жене);

– сведения о трудовой деятельности;

– данные о трудовом договоре (контракте) (№ трудового договора (контракта), дата его заключения, дата начала и дата окончания договора (контракта), вид работы, срок действия договора (контракта), наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору (контракту), характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);

– сведения о приеме на работу, перемещении по должности, увольнении;

– сведения об отпусках;

– сведения о командировках;

– сведения о временной нетрудоспособности[6];

– сведения о воинском учете и реквизиты документов воинского учета;

– сведения об образовании (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, направление подготовки или специальность, квалификация по документу об образовании);

– сведения о послевузовском профессиональном образовании (наименование и год окончания образовательной или научной организации), ученой степени, ученом звании (дата присвоения, номера дипломов, аттестатов);

– сведения о владении иностранными языками, степень владения;

– сведения о пребывании за границей (страна, год и цель пребывания), серия номер заграничного паспорта, наименование органа, выдавшего его, дата выдачи;

– сведения об оформленных допусках к государственной тайне (форма, номер и дата);

– сведения о профессиональной переподготовке и (или) повышении квалификации

– номер расчетного счета;

– номер банковской карты;

– занимаемая должность;

– иные персональные данные, предоставленные субъектом.

С персональными данными может производиться автоматизированная и неавтоматизированная обработка.

Также я даю/не даю (нужное подчеркнуть) согласие на включение в общедоступные источники информации такие как официальный сайт Администрации городского округа Щёлково с целью предоставления контактных сведений и информации о структуре посетителям официального сайта, следующих моих персональных данных: фамилия, имя, отчество, должность, номер телефона (нужное подчеркнуть).

Согласие действует в течение действия трудовых отношений и 3 года после их окончания.

Действие настоящего Согласия прекращается досрочно в случае принятия Оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

«____» _____ 20____ г. _____
(подпись)

---

[5] Не используется для идентификации субъекта

[6] В электронном виде обрабатывается только продолжительность больничного

Утвержден распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Перечень
информационных систем Администрации городского округа Щёлково

I. Основные положения

1.1. Настоящий перечень разработан в соответствии с требованиями Постановления Правительства Российской Федерации от 21 марта 2012 г. № 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».

1.2. В Администрации городского округа Щёлково функционируют следующие информационные системы:

№	Наименование информационной системы	Назначение информационной системы
1.	Информационная система персональных данных «Кадры» (ИСПДн «Кадры»)	– осуществление подбора персонала; – формирование кадрового состава для замещения должностей муниципальной службы; – организация кадрового делопроизводства Администрации; – подготовка и передача данных в контролирующие органы (ПФР, ФСС, ФНС, Росстат и прочие) в соответствии с требованиями законодательства, а также по запросу государственных органов; – осуществление деятельности по профилактике коррупционных и иных правонарушений

Утверждена распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Форма разъяснения юридических последствий отказа предоставить свои персональные данные

Мне, _____ разъяснены
(фамилия, имя, отчество)
юридические последствия отказа предоставить свои персональные данные Администрации городского округа Щёлково, расположенной по адресу: г. Щёлково, пл. Ленина, д. 2. В соответствии со статьями 16, 29 Федерального закона от 02 марта 2007 года № 25-ФЗ «О муниципальной службе в Российской Федерации» определен перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с поступлением на муниципальную службу.

Без представления субъектом персональных данных обязательных для заключения трудового договора (контракта) сведений, трудовой договор (контракт) не может быть заключен.

«___» _____ 20___ г. _____
(подпись)

Утверждены распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Формы запросов, разъяснений, отказов, связанных с рассмотрением запросов субъектов персональных данных или их представителей

_____
(должность руководителя)

_____
(наименование организации)

_____
(ФИО руководителя)

От _____
(фамилия, имя, отчество полностью)

проживающего по адресу_____

_____

_____

паспорт серия _____ номер _____

_____

_____
(кем и когда выдан)

Запрос №_____
на предоставление сведений, касающихся персональных данных

На основании статьи 14 главы 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» прошу предоставить следующие сведения (выделить нужное):

подтверждение факта обработки персональных данных оператором, а также цель такой обработки;

способы обработки персональных данных, применяемые оператором;

сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

перечень обрабатываемых персональных данных и источник их получения;

сроки обработки персональных данных, в том числе сроки их хранения;

сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;

другое:

_____

_____

_____ _____
(дата) *(подпись)*

_____
(должность руководителя)

_____
(наименование организации)

_____
(ФИО руководителя)

От _____
(фамилия, имя, отчество полностью)

проживающего по адресу_____

_____

_____

паспорт серия _____ номер _____

_____

_____
(кем и когда выдан)

Запрос №____
на блокирование, удаление, уточнение персональных данных

Прошу _____ мои персональные данные
(блокировать/удалить/уточнить)
по следующим причинам (нужное выделить):

персональные данные являются неполными;

персональные данные являются устаревшими;

персональные данные являются недостоверными;

персональные данные являются незаконно полученными;

персональные данные не являются необходимыми для заявленной цели обработки;

другое:

_____

_____

_____ _____
(дата) *(подпись)*

_____
(фамилия, имя, отчество субъекта ПДн)

от_____

Уведомление № _____
о блокировании, удалении, уточнении персональных данных

Согласно запросу № _____ от _____ на _____
(дата запроса) *(блокирование/удаление/уточнение)*
персональных данных было произведено _____
(блокирование/удаление/уточнение)
Ваших персональных данных:
_____
(фамилия, имя, отчество)
проживающий по адресу: _____
_____
паспорт серия _____ номер _____ выдан
_____
_____
(кем и когда выдан)

_____ _____ _____
(должность исполнителя) *(фамилия, инициалы)* *(подпись)*
«___» _____ 20___ г.

_____
(фамилия, имя, отчество субъекта ПДн)

от_____

Уведомление № _____
об отказе блокирования, удаления, уточнения персональных данных

В запросе № _____ от _____ на _____
(дата запроса) *(блокирование/удаление/уточнение)*
Ваших персональных данных отказано по следующей причине:
_____
_____
_____
_____
_____

_____ _____ _____
(должность исполнителя) *(фамилия, инициалы)* *(подпись)*
«___» _____ 20___ г.

_____
(фамилия, имя, отчество субъекта ПДн)

от_____

Уведомление № _____
о предоставлении сведений, касающихся персональных данных

Согласно запросу № _____ от _____ на получение сведений,
(дата запроса)
касающихся персональных данных, и на основании статьи 14 главы 3 Федерального закона от 27 июля 2006 года 152-ФЗ «О персональных данных» Вам предоставляется следующая информация:

Цель обработки персональных данных:
_____
_____

Способы обработки персональных данных:
_____
_____

Перечень информационных систем, в которых обрабатываются персональные данные:
_____
_____

Лица, имеющие доступ к персональным данным, и лица, которым может быть предоставлен такой доступ:
_____
_____
_____

Перечень обрабатываемых персональных данных и источник их получения:
_____
_____
_____
_____

Сроки обработки персональных данных, сроки хранения персональных данных:
_____
_____
_____
_____
_____

_____ _____ _____
(должность исполнителя) *(фамилия, инициалы)* *(подпись)*

«___» _____ 20___ г.

_____
(фамилия, имя, отчество субъекта ПДн)

от_____

Уведомление № _____
об отказе в предоставлении сведений, касающихся персональных данных

В запросе № _____ от _____ на получение сведений,
(дата запроса)
касающихся Ваших персональных данных, отказано по следующей причине:

☐ на основании пункта 5 статьи 14 главы 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

– обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

– обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

– предоставление персональных данных нарушает конституционные права и свободы других лиц.

☐ запрос субъекта персональных данных (или его законного представителя) содержит неполную или недостоверную информацию о субъекте, или его законном представителе.

☐ в запросе субъекта персональных данных содержится требование предоставить персональные данные, относящиеся к другим субъектам персональных данных.

_____ _____ _____
(должность исполнителя) *(фамилия, инициалы)* *(подпись)*

«___» _____ 20___ г.

Утверждено распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

ФОРМА

Соглашение о неразглашении персональных данных

Я,_____,
(фамилия, имя, отчество)
зарегистрированный(ая) по адресу:_____
_____паспорт серия _____
номер _____, выдан_____
_____
(кем и когда)

предупрежден(а) о том, что на период исполнения мною должностных обязанностей по Трудовому договору (контракту), заключенному между мною и Администрацией городского округа Щёлково (далее – Оператор), предусматривающих работу с персональными данными, мне будет предоставлен доступ к информации ограниченного доступа в соответствии с организационно-распорядительными документами, утвержденными Оператором.

Настоящим добровольно принимаю на себя обязательства:

– не передавать (в любом виде) и не разглашать третьим лицам и сотрудникам Оператора, не имеющим на это право в силу выполняемых ими должностных обязанностей или в соответствии с решением руководства Оператора, персональные данные, обрабатываемые в информационных системах Оператора (за исключением собственных данных), которые мне доверены (будут доверены) или станут известными в связи с исполнением должностных обязанностей;

– в случае попытки третьих лиц или сотрудников Оператора, не имеющих на это право, получить от меня персональные данные, обрабатываемые Оператором, немедленно сообщать об этом факте ответственному за организацию обработки персональных данных;

– не использовать персональные данные, обрабатываемые Оператором, с целью получения выгоды;

– выполнять требования закона и иных нормативных правовых актов Российской Федерации, а также внутренних документов Оператора, регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;

– после прекращения моих прав на допуск к персональным данным, обрабатываемым Оператором, (переход на должность, не предусматривающую доступ к персональным данным или прекращение Трудового договора), не разглашать и не передавать третьим лицам и неуполномоченным на это сотрудникам Оператора, известные мне персональные данные.

Я предупрежден(а) о том, что в случае нарушения данных обязательств буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с действующим законодательством Российской Федерации.

_____ _____ «___» _____ 20___ г.
(фамилия, инициалы) *(подпись)*

Утверждены распоряжением
Администрации
городского округа Щёлково
от 18.12.2020 № 340-р

Правила
рассмотрения запросов субъектов персональных данных или их представителей

I. Общие положения

1.1. Настоящие правила разработаны в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.2. В данном документе представлены правила рассмотрения запросов субъектов персональных данных (далее – ПДн) или их представителей.

1.3. Организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и контроль за приемом и обработкой таких обращений и запросов возлагается на ответственного за организацию обработки персональных данных.

II. Порядок предоставления ПДн

2.1. ПДн предоставляются субъекту или его законному представителю при обращении или поступлении соответствующего Запроса на предоставление персональных данных. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта (или его законного представителя), сведения о дате выдачи указанного документа и выдавшем его органе, сведения (номер договора, дата заключения договора, условное обозначение и (или) иные сведения), подтверждающие участие субъекта в отношениях с Администрацией городского округа Щёлково (далее – Оператор). Запрос может быть направлен в электронной форме и подписан электронной подписью в соответствии с законодательством Российской Федерации.

2.2. ПДн должны быть представлены субъекту или его законному представителю Оператором в доступной форме, и не должны содержать ПДн, относящиеся к другим субъектам ПДн. Помимо своих основных ПДн субъекту по его требованию должна быть предоставлена следующая информация:

- подтверждение факта обработки ПДн Оператором;
- правовые основания и цели обработки ПДн;
- цели и способы обработки ПДн Оператором;
- наименование и местонахождение Оператора, сведения о лицах (за исключением сотрудников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании федерального закона;

– обрабатываемые ПДн, относящиеся к субъекту, а также источник их получения (если иной порядок представления таких данных не предусмотрен федеральным законом);

– сроки обработки и хранения ПДн;

– порядок осуществления субъектом прав, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– наименование или фамилию, имя, отчество и адрес лица, которое осуществляет обработку ПДн по поручению Оператора (если обработка поручается такому лицу);

– иные сведения, предусмотренные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» или другими федеральными законами.

2.3. Ответственный за организацию обработки персональных данных фиксирует в Журнале учета обращений субъектов персональных данных о выполнении их законных прав при обработке персональных данных в информационных системах персональных данных факт поступления запроса, а также результат его рассмотрения.

2.4. Оператор обязан в порядке, предусмотренном п. 2 настоящего документа, сообщить субъекту (или его законному представителю) информацию о наличии ПДн, относящихся к данному субъекту, а также предоставить возможность ознакомления с ними при обращении субъекта (или его законного представителя) в течение тридцати дней с даты получения запроса субъекта (или его законного представителя).

2.5. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с момента получения такого запроса.

2.6. В случае отказа субъекту (или его законному представителю) в предоставлении ПДн или информации о наличии ПДн о соответствующем субъекте ПДн при их обращении (при получении запроса) Оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения (с даты получения запроса) субъекта (или его представителя).

2.7. Оператор обязан:

– безвозмездно предоставить субъекту или его законному представителю возможность ознакомления с ПДн, относящимися к

соответствующему субъекту ПДн, а также внести в них необходимые изменения в срок, не превышающий семи рабочих дней;

– уничтожить соответствующие ПДн в срок, не превышающий семи рабочих дней с момента предоставления субъектом (или его законным представителем) сведений, подтверждающих, что ПДн, которые относятся к данному субъекту и обработку которых осуществляет Оператор, являются неполными, неточными, неактуальными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– уведомить субъекта или его законного представителя и третьих лиц, которым ПДн этого субъекта были переданы о внесенных изменениях и предпринятых мерах.

2.8. Факт предоставления ПДн субъекту (или его законному представителю) должен фиксироваться в Журнале учета обращений субъектов персональных данных о выполнении их законных прав при обработке персональных данных в информационных системах персональных данных.

III. Порядок приостановки предоставления ПДн в случае обнаружения нарушений

3.1. В случае выявления неправомерной обработки ПДн при обращении (по запросу) субъекта (или его представителя) либо уполномоченного органа по защите прав субъектов ПДн Оператор обязан осуществить блокирование неправомерно обрабатываемых ПДн, которые относятся к данному субъекту, или обеспечить их блокирование (если обработка ПДн осуществляется третьим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки.

3.2. В случае выявления неточных ПДн при обращении (по запросу) субъекта (или его представителя) или по запросу уполномоченного органа по защите прав субъектов ПДн Оператор обязан осуществить блокирование ПДн, которые относятся к данному субъекту, или обеспечить их блокирование (если обработка ПДн осуществляется третьим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта или третьих лиц.

3.3. В случае подтверждения факта неточности ПДн Оператор на основании сведений, представленных субъектом (или его представителем) либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязан уточнить ПДн либо обеспечить их уточнение (если обработка ПДн осуществляется третьим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.

3.4. В случае выявления неправомерной обработки ПДн, осуществляемой Оператором (или лицом, действующим по его поручению), Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн. Если обеспечить правомерность обработки ПДн невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Оператор обязан уведомить субъекта (или его представителя), а также уполномоченный орган по защите прав субъектов ПДн (в случае, если обращение (запрос) было направлено указанным органом).

3.5. В случае достижения цели обработки ПДн Оператор обязан прекратить обработку ПДн (или обеспечить ее прекращение) и уничтожить ПДн (или обеспечить их уничтожение) в срок, не превышающий тридцати дней с даты достижения цели обработки, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект, и иным соглашением между Оператором и субъектом, либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта на основаниях, предусмотренных Федеральным законом» от 27 июля 2006 года № 152-ФЗ «О персональных данных» или другими федеральными законами.

3.6. В случае отзыва субъектом согласия на обработку его ПДн Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки. В случае если сохранение ПДн более не требуется для целей обработки ПДн, Оператор обязан уничтожить ПДн или обеспечить их уничтожение в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект, иным соглашением между Оператором и субъектом либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта на основаниях, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» или другими федеральными законами. Оператор вправе продолжить обработку ПДн субъекта при наличии оснований, указанных в пунктах 2 – 11 части 1 статьи 6, части 2 статьи 10 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

3.7. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 3.4 – 3.6, Оператор осуществляет блокирование таких ПДн или обеспечивает их блокирование и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.