



АДМИНИСТРАЦИЯ ГОРОДА МАГНИТОГОРСКА ЧЕЛЯБИНСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

20.08.2021

№ 271 - Р

Об утверждении перечня документов,
направленных на обеспечение
безопасности персональных данных
в администрации города Магнитогорска

В соответствии с Федеральным законом «О персональных данных», постановлениями Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», руководствуясь Уставом города Магнитогорска,

СЧИТАЮ НЕОБХОДИМЫМ:

1. Утвердить перечень документов, направленных на обеспечение безопасности персональных данных в администрации города Магнитогорска:

1) правила обработки персональных данных в администрации города Магнитогорска (приложение № 1);

2) правила рассмотрения запросов субъектов персональных данных или их представителей в администрации города Магнитогорска (приложение № 2);

3) правила работы с обезличенными данными в случае обезличивания персональных данных в администрации города Магнитогорска (приложение № 3);

4) перечень информационных систем администрации города, в которых происходит обработка персональных данных, в администрации города Магнитогорска (приложение № 4);

5) перечень персональных данных, обрабатываемых в связи с реализацией служебных и трудовых отношений, а также в связи с оказанием муниципальных услуг и осуществлением муниципальных функций в администрации города Магнитогорска (приложение № 5);

6) перечень должностей в администрации города Магнитогорска, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных (приложение № 6);

7) типовое обязательство муниципального служащего или работника, занимающего должность, не отнесенную к должности муниципальной

службы, и осуществляющего техническое обеспечение деятельности администрации города Магнитогорска, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного договора о прекращении обработки персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (приложение № 7);

8) порядок доступа работников администрации города Магнитогорска в помещения, в которых ведется обработка персональных данных (приложение № 8);

9) порядок уничтожения персональных данных при достижении целей обработки или наступлении иных законных оснований в администрации города Магнитогорска (приложение № 9);

10) обязательство о неразглашении конфиденциальной информации (персональных данных), не содержащих сведений, составляющих государственную тайну (приложение № 10);

11) согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения (приложение № 11);

12) согласие на обработку персональных данных (приложение № 12);

13) журнал учета стационарных машинных носителей информации (приложение № 13);

14) журнал учета съемных машинных носителей информации (приложение № 14);

15) журнал учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных (приложение № 15);

16) журнал учета паролей пользователей (приложение № 16);

17) журнал учета средств защиты информации (приложение № 17);

18) журнал учета хранилищ персональных данных (приложение № 18);

19) журнал учета персональных идентификаторов и электронных ключей (приложение № 19);

20) инструкция ответственного за обеспечение безопасности персональных данных в администрации города Магнитогорска (приложение № 20);

21) инструкция по физической охране, контролю доступа в помещения, в которых ведется обработка персональных данных в администрации города Магнитогорска (приложение № 21);

22) инструкция пользователей информационной системы персональных данных в администрации города Магнитогорска (приложение № 22);

23) инструкция администратора по техническому обеспечению безопасности персональных данных в администрации города Магнитогорска (приложение № 23);

24) инструкция по резервному копированию и восстановлению информационных ресурсов в администрации города Магнитогорска (приложение № 24);

25) инструкция об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации в администрации города Магнитогорска (приложение № 25);

26) правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации города Магнитогорска (приложение № 26);

27) инструкция по организации парольной защиты и защиты от несанкционированного доступа на объектах информатизации в администрации города Магнитогорска (приложение № 27);

28) инструкция по организации антивирусной защиты в администрации города Магнитогорска (приложение № 28);

29) журнал учета выявленных инцидентов информационной безопасности (приложение № 29);

30) журнал поэкземплярного учета средств криптографической защиты информации, технической и эксплуатационной документации к ним (приложение № 30).

2. Настоящее распоряжение вступает в силу с 01.01.2022, за исключением подпунктов 11 и 12 пункта 1, которые вступают в силу со дня подписания настоящего распоряжения.

3. Руководителям органов администрации города Магнитогорска ознакомить работников с настоящим распоряжением.

4. Контроль исполнения настоящего распоряжения возложить на заместителя главы города – руководителя аппарата администрации города Москалева М.В.

Глава города



С.Н. Бердников

ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ ГОРОДА МАГНИТОГОРСКА

I. Общие положения

1. Правила обработки персональных данных (далее – Правила) в администрации города Магнитогорска (далее – администрация города) (далее – оператор) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных, а также определяют для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

2. Обработка персональных данных в администрации города выполняется с использованием средств автоматизации и без использования таких средств и включает: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3. Правила определяют политику администрации города как оператора, осуществляющего обработку персональных данных и определяющего цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

4. Субъектами персональных данных являются:

- 1) юридические лица;
- 2) физические лица, претендующие на получение грамоты награждению главы города с денежным вознаграждением;
- 3) индивидуальные предприниматели;
- 4) обучающиеся, родители, педагогические работники;
- 5) несовершеннолетние и законные представители несовершеннолетних;
- 6) служащие, работники, занимающие должность, не отнесенную к должности муниципальной службы, и осуществляющие техническое обеспечение деятельности администрации города, работники, занятые обслуживанием администрации города, а также граждане, претендующие на замещение вакантных должностей муниципальной службы в администрации города;

7) работники администрации города, работники подведомственных учреждений культуры, физической культуры, здравоохранения;

8) инвалиды I, II, III групп, дети-инвалиды до 18-ти лет, инвалиды войны и приравненные к ним лица I, II, III групп, участники ВОВ, жители блокадного Ленинграда, члены семей погибших (умерших) военнослужащих, ветераны боевых действий, бывшие несовершеннолетние узники фашизма, граждане,

подвергшиеся воздействию радиации вследствие аварии на ЧАЭС, граждане, пострадавшие от деятельности ПО «МАЯК», граждане, подвергшиеся воздействию радиации вследствие ядерных испытаний на Семипалатинском полигоне, граждане из подразделений особого риска, почетный донор России, СССР, ветераны труда (пенсионеры), ветераны труда Челябинской области, ветераны военной службы (пенсионеры), реабилитированные лица, лица, пострадавшие от политических репрессий, труженики тыла, Герои социалистического труда, вдовы героев, кавалеры ордена Трудовой Славы, получатели субсидии на оплату жилья и коммунальных услуг, получатели ежемесячных детских пособий, получатели единовременных детских пособий, многодетные семьи, семьи с детьми под опекой, приемные семьи, граждане, пенсионного возраста, пенсионеры, не имеющие льгот;

9) организации, входящие в состав спасательных служб города Магнитогорска;

10) молодежь до тридцати пяти лет;

11) члены общественных организаций;

12) иные лица - заявители.

5. Обработка персональных данных в администрации города осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации в области персональных данных и настоящими Правилами.

II. Условия и порядок обработки персональных данных в связи с реализацией служебных или трудовых отношений

6. Персональные данные субъектов, указанных в пункте 4 настоящих Правил, обрабатываются в целях:

1) регистрации обращений и подготовки ответов, а также предоставления государственных муниципальных услуг;

2) контроля и управления муниципальным имуществом, осуществления контроля за своевременным поступлением арендных платежей;

3) сбора данных об участниках государственной итоговой аттестации (далее – ГИА), сбора данных ГИА (информация о пункте проведения экзамена (далее – ППЭ), аудиторном фонде, работниках ППЭ), выполнения работы по планированию работы ППЭ; постановки на учет и зачисления детей в образовательные учреждения, реализующие основную образовательную программу дошкольного образования; предоставления информации о текущей успеваемости учащегося в муниципальном образовательном учреждении, ведения электронного дневника и электронного журнала успеваемости; предоставления информации об образовательных программах и учебных планах, рабочих программах учебных курсов, предметах, дисциплинах (модулях), годовых календарных учебных графиках; организации аттестации, нормативного и кадрового обеспечения деятельности образовательных учреждений; направления ответов на обращения граждан взаимодействия сотрудников с органом администрации города;

4) предоставления мер социальной поддержки населению города Магнитогорска;

5) предоставления услуг по государственной регистрации смерти и иных юридически значимых действий: выдача повторных документов из архива отдела ЗАГС, внесение исправлений, изменений в акты гражданского состояния, дооформление записей акта о расторжении брака, предоставление сведений о государственной регистрации актов гражданского состояния государственным учреждениям и истребование документов, актов гражданского состояния с территории иностранных государств.

6) начисления и удержаний из заработной платы, начисления и перечисления страховых взносов в государственные и негосударственные фонды, учета командировочных и хозяйственных расходов;

7) обеспечения законодательных и иных нормативных актов Российской Федерации; защиты жизни и здоровья или иных жизненно важных интересов субъектов персональных данных;

8) реализации городских целевых программ по поисковой деятельности в местах ведения боевых действий; по осуществлению мероприятий по работе с детьми и молодежью по нравственно-патриотическому воспитанию при организации летних полевых и военно-спортивных лагерей, походов и сплавов; по осуществлению участия представителей молодежи, коллективов, групп, команд, отрядов города в областных, межрегиональных, всероссийских, федеральных, международных предприятиях; для создания условий для самоопределения подрастающего поколения в выборе профессии, предоставление возможностей временного и постоянного трудоустройства детей и молодежи в летний период и в свободное от учебы время, обеспечения соблюдения законов и иных нормативных правовых актов, содействия физическим лицам в трудоустройстве, направления ответа на обращения граждан и взаимодействия с работниками органа администрации города;

9) экстренного реагирования при чрезвычайных ситуациях;

10) взаимодействия с подведомственными предприятиями и учреждениями;

11) обеспечения кадровой работы, в том числе в целях содействия в прохождении муниципальной службы, содействия в выполнении осуществляемой работы, формирования кадрового резерва муниципальной службы, обучения и должностного роста, учета результатов исполнения должностных обязанностей, обеспечения личной безопасности гражданских служащих, работников, замещающих отдельные должности, включая членов их семей, обеспечения установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества;

12) предоставление земельного участка для целей, не связанных со строительством;

13) отнесение земельного участка к категории земель – земли населенных пунктов;

14) предоставление гражданину земельного участка, составляющего территорию садоводческого (огороднического) некоммерческого товарищества для ведения садоводства (огородничества);

15) выдача повторных свидетельств о государственной регистрации актов гражданского состояния и иных документов, подтверждающих факты государственной регистрации актов;

16) государственная регистрация актов гражданского состояния;

17) истребование и пересылка документов о государственной регистрации;

18) управления развитием территории города, хозяйственными процессами и комплексами объектов;

19) рассмотрение заявлений физических и юридических лиц о предоставлении земельных участков для целей, не связанных со строительством (временное размещение объектов, не являющихся объектами капитального строительства);

20) оформление и согласование соответствующих документов по результатам рассмотрения заявлений физических и юридических лиц о предоставлении земельных участков для целей, не связанных со строительством;

21) рассмотрение обращений физических и юридических лиц о размещении объектов благоустройства и озеленения на территориях общего пользования районов города;

22) рассмотрение обращений членов садоводческих, огороднических или дачных некоммерческих объединений граждан, по подготовке проектов постановлений администрации города, связанных с оформлением садовых, огородных, дачных земельных участков;

23) рассмотрение письменных обращений и заявлений граждан района по вопросам жилищно-коммунального хозяйства, в части использования земельных участков, торговли, потребительского рынка;

24) организация работы с руководителями территориальных общественных самоуправлений и председателями квартальных комитетов поселков;

25) ведение учета домовладений индивидуальных жилых застроек населения;

26) работа с общественными организациями по направлениям деятельности;

27) выдача справок гражданам, удостоверяющие юридически значимые факты, связанные с местом их проживания;

28) прием, регистрация и передача по назначению входящей корреспонденции;

29) организация приема граждан главой города и главами районных администраций;

30) работа с обращениями граждан (прием, регистрация, подготовка ответа);

31) составление графиков очередных отпусков;

32) оформление грамот и благодарственных писем;

33) ведение синтетического и аналитического учета расчетов с работниками администрации города, района, удержания из заработной платы, начислений и перечислений налогов на заработную плату;

34) учет командировочных и хозяйственных расходов;

35) осуществление государственной регистрации рождения, заключения брака, расторжения брака, усыновления (удочерения), установления отцовства, перемены имени, смерти;

36) прием документов, необходимых для государственной регистрации актов гражданского состояния;

37) осуществление расторжения брака, аннулирования записей актов гражданского состояния на основании решений судов.

7. В целях, указанных в пункте 6 настоящих Правил, обрабатываются следующие категории персональных данных субъектов персональных данных, указанных в пункте 4 настоящих Правил:

1) фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

2) число, месяц, год рождения;

3) место рождения;

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

5) адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;

6) номер контактного телефона или сведения о других способах связи;

7) реквизиты страхового свидетельства обязательного пенсионного страхования;

8) идентификационный номер налогоплательщика.

9) сведения о состоянии здоровья

10) сведения о льготах;

11) средний балл ученика;

12) сведения о семейном положении, составе семьи и о близких родственниках (в том числе бывших);

13) сведения о трудовой деятельности;

14) сведения о воинском учете и реквизиты документов воинского учета;

15) сведения об образовании (когда и какие образовательные, научные и иные организации окончил, номера документов об образовании, направление подготовки или специальность по документу об образовании, квалификация);

16) сведения об ученой степени;

17) сведения, содержащиеся в служебном контракте (трудовом договоре), дополнительных соглашениях к служебному контракту (трудовому договору);

18) сведения о датах рождения детей;

19) сведения о государственных наградах, иных наградах и знаках отличия;

20) сведения о профессиональной переподготовке и (или) повышении квалификации;

21) сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

22) документы, дающие право на меры социальной поддержки;

23) полис обязательного медицинского страхования;

24) справка о доходе семьи;

24) военный билет;

25) трудовая книжка;

26) пенсионное удостоверение;

- 27) свидетельство о браке;
- 28) свидетельство о смерти;
- 29) сведения о заработной плате;
- 30) номер лицевого счета, открытого в кредитной организации;
- 31) выписка из акта медицинского освидетельствования;
- 32) справка медико-социальной экспертизы, врачебно-трудовой экспертной комиссии;
- 33) исполнительный судебный лист;
- 34) решение суда, определение суда;
- 35) сведения о трудовом стаже и месте работы;
- 36) справки об обучении ребенка в общеобразовательном учреждении;
- 37) решение органа местного самоуправления об установлении над несовершеннолетним опеки (попечительства);
- 38) договора об осуществлении опеки (попечительства);
- 39) разрешение на временное проживание и документ, подтверждающих наличие трудовых отношений, для иностранных граждан и лиц без гражданства, временно проживающих на территории РФ;
- 40) Ф.И.О. умершего и заявителя, дата и место рождения, дата и место смерти, место жительства умершего и заявителя;
- 41) паспортные данные умершего и заявителя;
- 42) информация об имущественных отношениях;
- 43) должность;
- 44) стаж работы;
- 45) реквизиты свидетельства государственной регистрации актов гражданского состояния;
- 46) информация по 2-НДФЛ и 3-НДФЛ; документы, подтверждающие родственные связи (свидетельство об установлении отцовства, свидетельство о рождении, свидетельство о заключении и (или) расторжении брака); информация о группе инвалидности, коде заболевания по МКБ-10;
- 47) сведения о владении иностранными языками, уровень владения;
- 48) сведения об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению;
- 49) фотография;
- 50) сведения о прохождении муниципальной службы (работы), в том числе: дата, основания поступления на муниципальную службу (работу) и назначения на должность муниципальной службы, дата, основания назначения, перевода, перемещения на иную должность муниципальной службы (работы), наименование замещаемых должностей муниципальной службы с указанием структурных подразделений, размера денежного содержания (зарботной платы), результатов аттестации на соответствие замещаемой должности муниципальной службы, а также сведения о прежнем месте работы;
- 51) сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;
- 52) сведения о пребывании за границей;
- 53) сведения о классном чине муниципальной службы Российской Федерации (дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской,

муниципальной службы субъекта Российской Федерации), квалификационном разряде гражданской, муниципальной службы (квалификационном разряде или классном чине муниципальной службы);

54) сведения о наличии или отсутствии судимости;

55) сведения об оформленных допусках к государственной тайне;

56) номер банковской карты;

57) номер расчетного счета.

8. Обработка персональных данных субъектов, указанных в пункте 4 настоящих Правил, осуществляется без согласия указанных граждан в рамках целей, определенных пунктом 6 настоящих Правил, в соответствии со статьей 6 Федерального закона «О персональных данных», Федерального закона «О противодействии коррупции», Федерального закона «О муниципальной службе в Российской Федерации», Трудовым кодексом Российской Федерации.

9. Обработка персональных данных субъектов, указанных в пункте 4 настоящих Правил осуществляется при условии получения согласия указанных граждан в следующих случаях:

1) при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации о муниципальной службе;

2) при принятии решений, порождающих юридические последствия в отношении указанных граждан или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

10. Согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом "О персональных данных".

11. Обработка и использование персональных данных осуществляется в информационной системе персональных данных (далее – ИСПДн) администрации города.

12. В случае возникновения необходимости получения персональных данных субъектов у третьей стороны, следует заранее известить об этом субъектов персональных данных, получить их письменное согласие и сообщить им о целях, предполагаемых источниках и способах получения персональных данных.

13. Запрещается обрабатывать персональные данные, не предусмотренные приложением № 5 к настоящему распоряжению, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

14. При сборе персональных данных оператор обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

15. Обработка и использование персональных данных осуществляется в случаях и порядке, предусмотренных законодательством Российской Федерации.

III. Порядок обработки персональных данных

16. Оператору, имеющему право осуществлять обработку персональных данных на автоматизированных рабочих местах и в информационной системе, содержащие персональные данные, предоставляется уникальный логин и пароль для доступа к соответствующим данным.

17. Обеспечение безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах и в информационной системе, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

IV. Сроки обработки и хранения персональных данных

18. В соответствии с законодательством Российской Федерации определяются и устанавливаются сроки обработки и хранения персональных данных субъектов: персональные данные, содержащиеся в информационной системе, в которой обрабатываются персональные данные и на автоматизированных рабочих местах подлежат обязательному хранению на сервере до момента вывода из эксплуатации информационной системы.

20. Персональные данные граждан, обратившихся в орган администрации города лично, а также направивших письменные обращения или обращения в форме электронного документа, хранятся в течение 5 лет.

21. Персональные данные, предоставляемые на бумажном носителе в установленных законодательством случаях, хранятся у работников администрации города, включенных в перечень должностей, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей.

22. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на разных материальных носителях персональных данных.

23. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в целях, определенных настоящими Правилами.

V. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

24. Оператором осуществляется систематический контроль и выделение документов, содержащих персональные данные с истекшими сроками хранения, подлежащих уничтожению.

25. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании постоянно действующей технической комиссии по защите информации (далее – ПДТК).

По итогам заседания ПДТК составляется протокол и акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами ПДТК и утверждается начальником органа администрации города.

26. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

VI. Ответственные за организацию обработки персональных данных

33. Функции по обеспечению безопасности персональных данных в администрации города регулируются Распоряжением администрации города «О возложении функций по обеспечению безопасности персональных данных в администрации города Магнитогорска». Ответственность за обеспечение безопасности персональных данных в органах администрации города возложена на руководителей органов администрации города и лиц, назначенных ответственными за обработку персональных данных. Контроль и методическое сопровождение за организацией и обеспечением безопасности персональных данных в администрации города осуществляет орган, на который возложены функции по обеспечению информационной безопасности.

34. Ответственные за обработку персональных данных в своей работе руководствуются законодательством Российской Федерации в области персональных данных и настоящими Правилами.

35. Ответственные за обработку персональных данных в органах администрации города обязаны:

- 1) организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в органе администрации города, от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий;

- 2) осуществлять внутренний контроль за соблюдением требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

- 3) доводить до сведения уполномоченных на обработку персональных данных положения законодательства Российской Федерации в области персональных данных, локальные акты по вопросам обработки персональных данных, требования к защите персональных данных;

- 4) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений;

- 5) в случае нарушения требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

36. Ответственные за обработку персональных данных в органах администрации города вправе иметь доступ к информации, касающейся обработки персональных данных и включающей:

- 1) цели обработки персональных данных;
- 2) категории обрабатываемых персональных данных;

- 3) категории субъектов персональных данных, персональные данные которых обрабатываются;
- 4) правовые основания обработки персональных данных;
- 5) перечень действий с персональными данными, общее описание используемых в органе администрации города способов обработки персональных данных;
- 6) описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- 7) дату начала обработки персональных данных;
- 8) срок или условия прекращения обработки персональных данных;
- 9) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- 10) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

37. Руководители органов администрации города несут ответственность за ненадлежащее выполнение функций по организации обработки персональных данных в органах администрации города в соответствии с законодательством Российской Федерации, а также в соответствии с Распоряжением администрации города «О возложении функций по обеспечению безопасности персональных данных в администрации города Магнитогорска»

**ПРАВИЛА
РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ
ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ В АДМИНИСТРАЦИИ
ГОРОДА МАГНИТОГОРСКА**

1. В соответствии с частью 7 статьи 14 Федерального закона «О персональных данных» субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (далее – сведения). Субъект персональных данных вправе требовать от администрации города уточнения его персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме. В них не должны содержаться персональные данные, относящиеся к другим субъектам.

3. Сведения предоставляются субъекту персональных данных (его представителю) при его обращении либо при получении от него или его представителя запроса. Запрос должен содержать:

- 1) номер основного документа, удостоверяющего личность субъекта персональных данных (его представителя);
- 2) сведения о дате выдачи указанного документа и выдавшем его органе;
- 3) сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором, либо сведения, иным образом подтверждающие факт обработки персональных данных оператором;
- 4) подпись субъекта персональных данных (его представителя).

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4. Субъект персональных данных вправе обратиться повторно в администрацию города или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона «О персональных данных», а также в целях ознакомления с обрабатываемыми персональными данными в случае, если такие сведения или обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

5. В случае, если сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений,

указанных в части 7 статьи 14 Федерального закона «О персональных данных», и ознакомления с такими персональными данными 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 персональных данных.

6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего требованиям, предусмотренным пунктом 4, 5 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ В СЛУЧАЕ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ ГОРОДА МАГНИТОГОРСКА

I. Общие положения

1. Настоящий документ подготовлен в целях реализации Федерального закона «О персональных данных», Постановления Правительства Российской Федерации от 21.03.2012 № 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 и устанавливает правила работы с обезличенными данными, содержащимися в администрации города.

2. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

II. Термины и определения

3. Понятия, используемые в настоящих правилах, применяются в том значении, в каком они используются в Федеральном законе «О персональных данных».

III. Условия обезличивания

4. Обезличивание персональных данных может быть проведено с целью снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационной системы персональных данных в органе администрации города и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральными законами.

5. Способы обезличивания при условии дальнейшей обработки персональных данных:

- 1) уменьшение перечня обрабатываемых сведений;
- 2) замена части сведений идентификаторами;
- 3) обобщение – понижение точности некоторых сведений;
- 4) понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);
- 5) деление сведений на части и обработка в разных информационных системах.

6. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

IV. Правила работы с обезличенными персональными данными

7. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

8. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

9. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- 1) парольной политики;
- 2) антивирусной политики;
- 3) правил работы со съемными носителями (если они используются);
- 4) правил резервного копирования;
- 5) правил доступа в помещения, где ведется обработка персональных данных.

10. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение правил доступа к ним и в помещения, где они хранятся.

V. Порядок обеспечения безопасности при обработке и хранении обезличенных данных, осуществляемых без использования средств автоматизации

11. В целях обеспечения сохранности документов, содержащих обезличенные данные, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться работниками органа администрации города, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

12. Работа с документами, содержащими обезличенные данные, как и работа со всеми документами, поступающими в администрацию города, организуются в соответствии с утвержденной инструкцией по ведению делопроизводства в администрации города.

13. Обезличенные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях данных (далее – материальные носители).

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

15. Использование типовых форм документов, характер информации в которых предполагает или допускает включение в них обезличенных данных (далее – типовая форма), если типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки обезличенных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта обезличенных данных, источник получения обезличенных данных, сроки обработки обезличенных

данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки обезличенных данных.

16. При несовместимости целей обработки обезличенных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку обезличенных данных отдельно от других зафиксированных на том же носителе обезличенных данных, должны быть приняты меры по обеспечению раздельной обработки обезличенных данных, в частности:

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

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

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

18. Уточнение обезличенных данных 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 носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

19. Обработка обезличенных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории обезличенных данных можно было определить места хранения обезличенных данных (материальных носителей) должны соблюдаться условия, обеспечивающие сохранность обезличенных данных и исключающие несанкционированный к ним доступ, для этого документы должны находиться в закрываемых на замок шкафах, сейфах, иных шкафах, имеющих запираемые блок-секции.

20. Не допускается без согласования начальника органа администрации города и ответственного за обеспечение безопасности персональных данных в органе администрации города формирование и хранение баз данных, содержащих обезличенные данные.

VI. Порядок обеспечения безопасности при обработке и хранении обезличенных данных, осуществляемых с использованием средств автоматизации

21. Обработка обезличенных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к обезличенным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение обезличенных данных, а также иных несанкционированных действий.

22. Организация режима обеспечения безопасности, где размещено оборудование, а также охрана помещений, в которых ведется работа с обезличенными данными, должны обеспечивать сохранность носителей обезличенных данных, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

23. Безопасность обезличенных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку обезличенных данных (далее – уполномоченное лицо). Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность и безопасность обезличенных данных при их обработке.

24. При обработке обезличенных данных должно быть обеспечено:

1) проведение мероприятий, направленных на предотвращение несанкционированного доступа к обезличенным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

2) своевременное обнаружение фактов несанкционированного доступа к обезличенным данным;

3) недопущение воздействия на технические средства автоматизированной обработки обезличенных данных, в результате которого может быть нарушено их функционирование;

4) возможность незамедлительного восстановления обезличенных данных, измененных, заблокированных или уничтоженных вследствие несанкционированного доступа к ним;

5) постоянный контроль за обеспечением уровня защищенности обезличенных данных.

25. Мероприятия по обеспечению безопасности обезличенных данных при их обработке в информационной системе включают в себя:

1) учет лиц, допущенных к работе с персональными данными в информационной системе;

2) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей обезличенных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности обезличенных данных или другим нарушениям, приводящим к снижению уровня защищенности обезличенных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

3) оператор при необходимости может разработать дополнительные нормативные акты по защите обезличенных данных.

26. За осуществление мероприятий по обеспечению безопасности обезличенных данных при их обработке отвечает ответственный за обеспечение безопасности персональных данных в органе администрации города.

27. Лица, доступ которых к обезличенным данным необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим обезличенным данным на основании списка, утвержденного оператором или уполномоченным лицом.

28. При обнаружении нарушений порядка обработки обезличенных данных оператор или уполномоченное лицо незамедлительно устраняет причины нарушений.

29. В целях обеспечения антивирусной защиты работа с персональными данными проводится в соответствии с инструкцией «По организации антивирусной защиты».

VII. Порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований

30. Информация, содержащая обезличенные данные и информация, содержащая персональные данные при достижении целей обработки, содержащие данные, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению в соответствии с действующим законодательством.

31. Уничтожение информации на электронных, магнитных и оптических носителях информации необходимо осуществлять путем стирания информации.

32. Ответственность за полноту, защищенность от уничтожения, изменение, блокирование, а также за совершение иных несанкционированных действий в отношении обезличенных данных несут работники, допущенные к этой работе в соответствии со своими должностными обязанностями. Контроль за выполнением этой работы осуществляют начальник органа администрации города, а также сотрудник, ответственный за обеспечение безопасности персональных данных в органе администрации города.

Приложение № 4 к распоряжению
администрации города
от 20.08.2021 № 241-Р

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ АДМИНИСТРАЦИИ ГОРОДА
МАГНИТОГОРСКА, В КОТОРЫХ ПРОИСХОДИТ ОБРАБОТКА
ПЕРСОНАЛЬНЫХ ДАННЫХ

№	Наименование информационных систем
1.	Автоматизированная информационная система «УИГМИ - Росреестр»
2.	Официальный сайт администрации города www.magnitogorsk.ru
3.	Муниципальная информационная система «ИнМета-МИС»
4.	Система документационного обеспечения управления «БОСС-Референт»
5.	Автоматизированная система документационного обеспечения управления «Docsvision»
6.	Автоматизированная информационная система «Доверие»
7.	Автоматизированная информационная система «Обращения граждан»
8.	Автоматизированная информационная система «Право»
9.	1С: Бухгалтерия государственного учреждения 8
10.	УСЗН Магнитогорского городского округа
11.	1С: Предприятие (приватизация)
12.	Электронный сервис «Государственная регистрация юр.лиц и индивидуальных предпринимателей» по форме Р038001
13.	Система управления персоналом «Босс – Кадровик»

**ПЕРЕЧЕНЬ
ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ
В СВЯЗИ С РЕАЛИЗАЦИЕЙ СЛУЖЕБНЫХ И ТРУДОВЫХ ОТНОШЕНИЙ,
А ТАКЖЕ В СВЯЗИ С ОКАЗАНИЕМ МУНИЦИПАЛЬНЫХ УСЛУГ
И ОСУЩЕСТВЛЕНИЕМ МУНИЦИПАЛЬНЫХ ФУНКЦИЙ
В АДМИНИСТРАЦИИ ГОРОДА МАГНИТОГОРСКА**

Наименование персональных данных	Способ обработки
1) фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения); 2) число, месяц, год рождения; 3) место рождения; 4) вид, серия, номер документа, удостоверяющего личность, дата выдачи, наименование органа, выдавшего его; 5) адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания; 6) номер контактного телефона или сведения о других способах связи; 7) реквизиты страхового свидетельства обязательного пенсионного страхования; 8) идентификационный номер налогоплательщика. 9) сведения о состоянии здоровья 10) сведения о льготах; 11) средний балл ученика; 12) сведения о семейном положении, составе семьи и о близких родственниках (в том числе бывших); 13) сведения о трудовой деятельности; 14) сведения о воинском учете и реквизиты документов воинского учета; 15) сведения об образовании (когда и какие образовательные, научные и иные организации окончил, номера документов об образовании, направление подготовки или специальность по документу об образовании, квалификация); 16) сведения об ученой степени; 17) сведения, содержащиеся в служебном контракте (трудовом договоре), дополнительных соглашениях к служебному контракту (трудовому договору); 18) сведения о наличии или отсутствии судимости;	Автоматизированный и неавтоматизированный способ обработки

19) сведения о государственных наградах, иных наградах и знаках отличия; 20) сведения о профессиональной переподготовке и (или) повышении квалификации; 21) сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания; 22) документы, дающие право на меры социальной поддержки; 23) полис обязательного медицинского страхования; 24) справка о доходе семьи; 24) военный билет; 25) трудовая книжка; 26) пенсионное удостоверение; 27) свидетельство о браке; 28) свидетельство о смерти; 29) сведения о заработной плате; 30) номер лицевого счета, открытого в кредитной организации; 31) выписка из акта медицинского освидетельствования; 32) Справка медико-социальной экспертизы, врачебно-трудовой экспертной комиссии; 33) исполнительный судебный лист; 34) решение суда, определение суда; 35) сведения о трудовом стаже и месте работы; 36) справки об обучении ребенка в общеобразовательном учреждении; 37) решение органа местного самоуправления об установлении над несовершеннолетним опеки (попечительства); 38) договора об осуществлении опеки (попечительства); 39) разрешение на временное проживание и документ, подтверждающих наличие трудовых отношений, для иностранных граждан и лиц без гражданства, временно проживающих на территории РФ; 40) Ф.И.О. умершего и заявителя, дата и место рождения, дата и место смерти, место жительства умершего и заявителя, 41) паспортные данные умершего и заявителя; 42) информация об имущественных отношениях; 43) должность; 44) стаж работы; 45) реквизиты свидетельства государственной регистрации актов гражданского состояния;	
--	--

46) сведения о воинском учете и реквизиты документов воинского учета; 47) сведения о владении иностранными языками, уровень владения; 48) сведения об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению; 49) фотография; 50) сведения о прохождении гражданской службы (работы), в том числе: дата, основания поступления на гражданскую службу (работу) и назначения на должность гражданской службы, дата, основания назначения, перевода, перемещения на иную должность гражданской службы (работы), наименование замещаемых должностей гражданской службы с указанием структурных подразделений, размера денежного содержания (зарботной платы), результатов аттестации на соответствие замещаемой должности гражданской службы, а также сведения о прежнем месте работы; 51) номер банковской карты; 52) сведения о пребывании за границей; 53) сведения о классном чине гражданской службы Российской Федерации (дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде гражданской службы (квалификационном разряде или классном чине муниципальной службы); 54) сведения о наличии или отсутствии судимости; 55) сведения об оформленных допусках к государственной тайне; 56) информация по 2-НДФЛ и 3-НДФЛ; документы, подтверждающие родственные связи (свидетельство об установлении отцовства, свидетельство о рождении, свидетельство о заключении и (или) расторжении брака); информация о группе инвалидности, коде заболевания по МКБ-10; 57) сведения о датах рождения детей; 58) сведения о доходах, расходах, об имуществе и обязательствах имущественного характера; 59) номер расчетного счета.	
---	--

ПЕРЕЧЕНЬ
ДОЛЖНОСТЕЙ В АДМИНИСТРАЦИИ ГОРОДА МАГНИТОГОРСКА,
ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ
ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Заместитель главы города;
2. Руководитель органа администрации города;
3. Глава администрации района;
4. Заместитель руководителя органа администрации города;
5. Заместитель главы администрации района.

Отдельные должности в структурных подразделениях администрации города, в случае, если на муниципальных служащих и работников администрации города, замещающих данные должности, возложены функции по обеспечению безопасности персональных или проведения мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных:

1. Эксперт;
2. Консультант;
3. Начальник подразделения в составе органа администрации города;
4. Начальник ЕДДС;
5. Заместитель начальника ЕДДС – старший оперативный дежурный;
6. Помощник оперативного дежурного – оператор 112;
7. Начальник курсов;
8. Руководитель группы;
9. Юрисконсульт;
10. Главный специалист;
11. Ведущий специалист;
12. Специалист I категории;
13. Специалист II категории;
14. Специалист по связям с общественностью;
15. Специалист по внутреннему контролю;
16. Специалист по закупкам;
17. Секретарь руководителя;
18. Старший инспектор;
19. Инспектор;
20. Ведущий инженер;
21. Инженер;
22. Главный аналитик;
23. Аналитик;
24. Старший экономист;
25. Ведущий экономист;
26. Экономист;

27. Ведущий бухгалтер;
28. Бухгалтер;
29. Ведущий архивист;
30. Делопроизводитель;
31. Программист;
32. Методист;
33. Оперативный дежурный;
34. Документовед;
35. Оператор ЭВиВМ;
36. Художник компьютерной графики;
37. Заведующий складом;
38. Техник;
39. Диспетчер.

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО МУНИЦИПАЛЬНОГО СЛУЖАЩЕГО
ИЛИ РАБОТНИКА, ЗАНИМАЮЩЕГО ДОЛЖНОСТЬ, НЕ ОТНЕСЕННУЮ
К ДОЛЖНОСТИ МУНИЦИПАЛЬНОЙ СЛУЖБЫ, И ОСУЩЕСТВЛЯЮЩЕГО
ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЕЯТЕЛЬНОСТИ
АДМИНИСТРАЦИИ ГОРОДА МАГНИТОГОРСКА, НЕПОСРЕДСТВЕННО
ОСУЩЕСТВЛЯЮЩЕГО ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ,
В СЛУЧАЕ РАСТОРЖЕНИЯ С НИМ СЛУЖЕБНОГО ДОГОВОРА
О ПРЕКРАЩЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ,
СТАВШИХ ИЗВЕСТНЫМИ ЕМУ В СВЯЗИ С ИСПОЛНЕНИЕМ
ДОЛЖНОСТНЫХ ОБЯЗАННОСТЕЙ

Я, _____,
(фамилия, имя, отчество)

обязуюсь прекратить обработку персональных данных, ставших мне известными
в связи с исполнением должностных обязанностей, в случае расторжения со
мной трудового договора.

В соответствии со статьей 7 Федерального закона «О персональных
данных» я уведомлен(а) о том, что операторы и иные лица, получившие доступ
к персональным данным, обязаны не раскрывать третьим лицам и не
распространять персональные данные без согласия субъекта персональных
данных, если иное не предусмотрено федеральным законом.

Ответственность, предусмотренная законодательством Российской
Федерации, мне разъяснена.

(дата)

(подпись)

ПОРЯДОК ДОСТУПА РАБОТНИКОВ АДМИНИСТРАЦИИ ГОРОДА МАГНИТОГОРСКА В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящий Порядок доступа в помещение, в котором ведется обработка персональных данных (далее – Порядок) разработан в соответствии с Федеральным законом «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 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».

2. Персональные данные относятся к конфиденциальной информации. Работники администрации города, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе, установлением правил доступа в помещения, где осуществляется обработка персональных данных.

4. В помещениях, выделенных для органов администрации города, в которых ведется обработка персональных данных, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

5. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

6. В помещении, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только работники администрации города, уполномоченные на обработку персональных данных. Посторонние посетители допускаются только в присутствии работников администрации города.

7. Ответственными за организацию доступа в помещение, в котором ведется обработка персональных данных, является ответственный за

обеспечение безопасности персональных данных в органе администрации города при их обработке.

8. Внутренний контроль за соблюдением порядка доступа в помещение, в котором ведется обработка персональных данных, проводится лицом ответственным за обеспечение безопасности персональных данных в органе администрации города при их обработке.

**ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ
ПРИ ДОСТИЖЕНИИ ЦЕЛЕЙ ОБРАБОТКИ ИЛИ ПРИ НАСТУПЛЕНИИ
ИНЫХ ЗАКОННЫХ ОСНОВАНИЙ В АДМИНИСТРАЦИИ
ГОРОДА МАГНИТОГОРСКА**

I. Общие положения

1. Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в администрации города, в целях реализации: Федерального закона «О персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства Российской Федерации от 21.03.2012 № 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.

**II. Порядок уничтожения информации, содержащей
персональные данные, при достижении целей обработки
или при наступлении иных законных оснований**

2. Информация, содержащая персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившая практическое значение, а также с истекшим сроком хранения), подлежит уничтожению в соответствии с законодательством.

Уничтожение документов производится в присутствии всех членов комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (состав комиссии утверждается приказом по органу администрации города).

Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

После уничтожения материальных носителей членами комиссии подписывается акт в трех экземплярах (Приложение № 1) делается запись в журналах их учета и регистрации, а также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__ (дата)».

3. Уничтожение информации на электронных носителях необходимо осуществлять путем стирания информации.

4. Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению в соответствии с действующим законодательством.

Перед уничтожением информации исполнитель сообщает специалисту по обеспечению безопасности персональных данных в администрации города. Делаются соответствующие отметки об уничтожении файлов в Журнале уничтожения носителей персональных данных (Приложение № 2).

Приложение №1
к Порядку уничтожения персональных
данных при достижении целей их обработки
или при наступлении иных законных оснований

Акт № _____
об уничтожении носителей, содержащих персональные данные

Комиссия в составе:

Председатель: _____

Члены комиссии: _____

провела отбор бумажных, электронных, магнитных и оптических носителей персональных данных и другой конфиденциальной информации (далее – носители) и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит гарантированному уничтожению и 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 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 комиссии: _____ / _____ /

Члены комиссии: _____ / _____ /
_____ / _____ /

Приложение №2
к Порядку уничтожения
персональных данных при достижении
целей их обработки или при наступлении
иных законных оснований

Журнал уничтожения носителей персональных данных

Начат _____
Окончен _____
Ответственный _____ (Ф.И.О.)
На _____ листах

№ п/п	Наименование информационной системы персональных данных, в которой уничтожаются персональные данные	Ф.И.О. субъекта, персональн ые данные которого подлежащие уничтожени ю	Обоснован ие уничтожен ия	Наименование файла, и его месторасполож ение	Дата уничто жения	Ф.И.О. и подпись Исполни теля	Ф.И.О. и подпись ответственн ого за обработку персональн ых данных
1	2	3	4	5	6	7	8

ОБЯЗАТЕЛЬСТВО

о неразглашении конфиденциальной информации
(персональных данных), не содержащих сведений,
составляющих государственную тайну

Я, _____,
(ФИО)

исполняющий (ая) должностные обязанности по занимаемой должности

(должность, наименование органа администрации города)

предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностной инструкцией, мне будет предоставлен доступ к конфиденциальной информации (персональным данным), не содержащим сведений, составляющих государственную тайну. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному руководителю.
4. Не использовать конфиденциальные сведения с целью получения выгоды.
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.
6. В течение года после прекращения права на доступ к конфиденциальным сведениям не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

(фамилия, инициалы)

(подпись, дата)

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ,
РАЗРЕШЕННЫХ СУБЪЕКТОМ ПЕРСОНАЛЬНЫХ ДАННЫХ
ДЛЯ РАСПРОСТРАНЕНИЯ

Настоящим я, _____,
(Ф.И.О. полностью)

проживающий по адресу

зарегистрирован

_____ (адрес полностью)

паспорт

_____ (серия, номер)

выдан

_____ « ____ » _____ года
(наименование органа, выдавшего паспорт)

руководствуясь Федеральным законом «О персональных данных», заявляю о согласии на распространение администрации города (далее – Оператор) моих персональных данных с целью обеспечение соблюдения законов и иных нормативных правовых актов, содействие субъекту персональных данных в трудоустройстве, обучении и продвижении по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества:

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению (да/нет)	Разрешаю к распространению неограниченному кругу лиц (да/нет)	Условия и запреты	Дополнительные условия
Общие персональные данные	Фамилия				
	Имя				
	Отчество				
	Год, месяц, дата рождения				
	Место рождения				
	Адрес				
	Семейное положение				
	Социальное положение				
	Образование				
	Профессия				

	Телефон				
	Иная информация				
Специальные категории персональных данных	Состояние здоровья				
	Сведения о судимости				
	Имущественное положение				
	Доходы				
	Иные сведения				
Визуальные персональные данные	Цветное фотографическое изображение лица				
	Голос				
	Фотоизображение рисунка вен ладони, полученного в диапазоне, близкого к инфракрасному				
	ДНК				
	Радужная оболочка глаз				
	Дактилоскопическая информация				
	Иные сведения				

Сведения об информационных ресурсах Оператора, посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действие с персональными данными
magnitogorsk.ru	Предоставление доступа неограниченному кругу лиц

Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования Оператор обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

« ____ » _____ 20__ года
число месяц

подпись

Ф.И.О

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящим я, _____,
(Ф.И.О. полностью)

проживающий по адресу

_____,
зарегистрирован

(адрес полностью)
паспорт

(серия, номер)
выдан

(наименование органа, выдавшего паспорт) «___» _____ года

представляю оператору - администрации города (г. Магнитогорск Челябинской области, пр. Ленина, д. 72) свои персональные данные в целях обеспечения соблюдения трудового законодательства и иных нормативно-правовых актов при содействии в трудоустройстве, обучении и продвижении по работе, обеспечения личной моей безопасности, текущей трудовой деятельности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Моими персональными данными является любая информация, относящаяся ко мне как к физическому лицу (субъекту персональных данных), указанная в трудовом договоре, личной карточке работника (унифицированная форма Т-2), трудовой книжке и (или) сведениях о трудовой деятельности и полученная в течение срока действия настоящего трудового договора, в том числе: мои фамилия, имя, отчество, год, месяц, дата и место рождения, гражданство, документы, удостоверяющие личность, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, адреса фактического места проживания и регистрации по месту жительства, почтовые и электронные адреса, номера телефонов, фотографии, сведения об образовании, профессии, специальности и квалификации, семейном положении и составе семьи, сведения об имущественном положении, доходах, задолженности, занимаемых ранее должностях и стаже работы, воинской обязанности; сведения о трудовом договоре и его исполнении (занимаемые должности, существенные условия труда, сведения об аттестации, повышении квалификации и профессиональной переподготовке, поощрениях и наказаниях, видах и периодах отпуска, временной нетрудоспособности, социальных льготах, командировании, рабочем времени и пр.), а также о других договорах (индивидуальной, коллективной материальной ответственности, ученических, оказания услуг и т. п.), заключаемых при исполнении трудового договора.

Своей волей и в своих интересах выражаю согласие на осуществление оператором - администрации города любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных целей, в том числе выражаю согласие на обработку без ограничения моих персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, предоставление,

Ф.И.О.

Приложение № 13
к распоряжению

администрации города

от 20.08.2021 № 244-Р

«наименование органа администрации»

администрации города Магнитогорска Челябинской области

Журнал учета стационарных машинных носителей информации

Начато:	
Окончено:	
Количество листов:	
Срок хранения:	5 лет

Приложение № 14
к распоряжению
администрации города
от 10.08.2020 № 241-Р

«наименование органа администрации»
администрации города Магнитогорска Челябинской области

Журнал учета съёмных машинных носителей информации

Начато:	
Окончено:	
Количество листов:	
Срок хранения:	5 лет

Приложение № 15 к распоряжению
администрации города
от 20.08.2021 № 241-р

«наименование органа администрации»
администрации города Магнитогорска Челябинской области

Журнал учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных

Начато:	
Окончено:	
Количество листов:	
Срок хранения:	5 лет

Приложение № 16 к распоряжению
администрации города
от 20.09.2024 № 244-Р

«наименование органа администрации»
администрации города Магнитогорска Челябинской области

**Журнал учета
паролей пользователей**

Начато:	
Окончено:	
Количество листов:	
Срок хранения:	5 лет

Приложение № 17 к распоряжению
администрации города
от 20.02.2011 № 284-Р

«наименование органа администрации»
администрации города Магнитогорска Челябинской области

Журнал учета средств защиты информации

Начато:	
Окончено:	
Количество листов:	
Срок хранения:	5 лет

Приложение № 18 к распоряжению
администрации города
от 26.08.2021 № 241-Г

«наименование органа администрации»

администрации города Магнитогорска Челябинской области

Журнал учета хранящихся персональных данных

Начато:	
Окончено:	
Количество листов:	
Срок хранения:	5 лет

Приложение № 19 к распоряжению
администрации города
от 20.08.2021 № 441-Р

«наименование органа администрации»
администрации города Магнитогорска Челябинской области

Журнал учета персональных идентификаторов и электронных ключей

Начато:	
Окончено:	
Количество листов:	
Срок хранения:	5 лет

Инструкция
ответственного за обеспечение безопасности
персональных данных в администрации города Магнитогорска

I. Общие положения

1. Данная инструкция определяет основные обязанности и права ответственного за обеспечение безопасности персональных данных в администрации города.

2. Ответственный за обеспечение безопасности персональных данных является штатным сотрудником органа администрации города и назначается приказом начальника органа администрации города.

3. В прямые служебные обязанности ответственного за обеспечение безопасности персональных данных в органе администрации города входит контроль выполнения требований и организационных мероприятий по обеспечению безопасности персональных данных дополнительно к своим непосредственным обязанностям.

4. Ответственный за обеспечение безопасности персональных данных - лицо, отвечающее за организацию и состояние процесса обработки персональных данных в администрации города.

5. Ответственный отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение соответствующих работ.

6. Ответственный в своей работе руководствуется Федеральным законом «О персональных данных», а также иными нормативными правовыми актами, действующими на территории Российской Федерации, настоящей инструкцией.

II. Обязанности ответственного за обеспечение безопасности
персональных данных

7. Знать перечень установленных в органе администрации города автоматизированных рабочих мест (далее – АРМ) и перечень задач, решаемых с их использованием.

8. Знать перечень программного обеспечения, установленного на автоматизированных рабочих местах.

9. Обеспечивать постоянный контроль выполнения работниками установленного комплекса мероприятий по обеспечению безопасности персональных данных.

10. Немедленно сообщать ответственному за обеспечение безопасности персональных данных в администрации города о попытках несанкционированного доступа к информации и техническим средствам вычислительной техники, а также принимать необходимые меры по устранению нарушений:

1) устанавливать причины, по которым стал возможным несанкционированный доступ;

- 2) устанавливать последствия, к которым привел несанкционированный доступ;
- 3) вести «Журнал регистрации попыток несанкционированного доступа»;
- 4) проводить инструктаж работникам органов администрации города, обрабатывающих персональные данные в связи с исполнением служебных обязанностей.

III. Права ответственного за обеспечение безопасности персональных данных

11. Требовать от работников органов администрации города, обрабатывающих персональные данные в связи с исполнением служебных обязанностей, исполнения установленных правил обработки информации.
12. Участвовать в проведении служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов информационной системы персональных данных.
13. Обращаться к ответственному за обеспечение безопасности персональных данных в органах администрации города с требованием прекращения работы на автоматизированных рабочих местах, содержащих персональные данные при несоблюдении установленных правил обработки информации и невыполнении требований по безопасности.

IV. Ответственность ответственного за обеспечение безопасности персональных данных

14. Ответственный несет персональную ответственность за:
 - 1) несоблюдение требований настоящей Инструкции,
 - 2) правильность и объективность принимаемых решений, качество и своевременность проводимых им работ по обеспечению безопасности персональных данных,
 - 3) за все действия, совершенные от имени его учетной записи в информационной системе персональных данных, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.
15. Ответственный при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

V. Действия при обнаружении попыток несанкционированного доступа

16. К попыткам несанкционированного доступа относятся:
 - 1) сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

2) действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к информационным системам персональным данным, при использовании учетной записи администратора или другого пользователя информационной системы персональных данных, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

17. При выявлении факта несанкционированного доступа ответственный обязан:

1) по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

2) доложить начальнику органа администрации города служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

3) известить ответственного за организацию обработки персональных данных и администратора безопасности о факте несанкционированного доступа.

Инструкция по физической охране, контролю доступа в помещения,
в которых ведется обработка персональных данных
в администрации города Магнитогорска

I. Общие положения

1. Данная инструкция регламентирует условия и порядок осуществления доступа лиц в помещения, в которых ведется обработка персональных данных в администрации города Магнитогорска (далее – администрация города), в целях обеспечения предотвращения несанкционированного доступа к персональным данным. При обеспечении доступа лиц в помещения, где ведется обработка персональных данных, соблюдаются требования по защите персональных данных.

2. Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности администрации города и определяет порядок допуска работников администрации города, работников иных организаций и учреждений, граждан в помещение.

3. Контроль за порядком обеспечения доступа лиц в помещения возлагается на ответственного за обеспечение безопасности персональных данных в органе администрации города.

4. Помещения и оборудование должны быть размещены таким образом, чтобы исключить возможность бесконтрольного проникновения в эти помещения и к этому оборудованию посторонних лиц.

5. Для исключения возможности бесконтрольного проникновения в помещения и к установленному в них оборудованию посторонних лиц, включая сотрудников других подразделений, двери кабинетов запираются на ключ.

II. Порядок доступа в помещения сотрудников и граждан

6. Не допускается нахождение посторонних лиц в помещениях, где ведется обработка персональных данных во вне рабочее время.

7. Нахождение физических лиц в помещениях, в которых ведется обработка персональных данных в администрации города допускается только в рабочее время в присутствии ответственного за обеспечение безопасности персональных данных в органе администрации города или в присутствии сотрудника, осуществляющего обработку персональных данных.

8. В помещения пропускаются беспрепятственно:

- 1) начальник органа администрации города;
- 2) ответственный за обеспечение безопасности персональных данных в органе администрации города;
- 3) администратор по защите персональных данных;
- 4) работники, имеющие допуск к работе с персональными данными с целью выполнения функциональных обязанностей;

5) физические лица, работники других подразделений администрации города, сотрудники сторонних организаций для выполнения договорных отношений в присутствии ответственного за обеспечение безопасности персональных данных в органе администрации города или в присутствии сотрудника, осуществляющего обработку персональных данных.

6) работники контролирующих органов;

7) работники пожарных и аварийных служб, сотрудники правоохранительных органов.

9. В помещениях, в которых происходит обработка и хранение персональных данных, запрещено использование не предусмотренных служебными обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

III. Организация и порядок производства ремонтно-строительных работ в здании

10. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных руководством. Работы проводятся только в присутствии в сопровождении ответственного за обеспечение безопасности персональных данных в органе администрации города или руководителя органа администрации города, или в присутствии сотрудника, осуществляющего обработку персональных данных.

11. Для предотвращения несанкционированного доступа к информации, содержащей персональные данные, следует контролировать деятельность работников, при необходимости, заблокировать персональный компьютер.

IV. Организация охраны

12. Режим работы охраны устанавливается штатным расписанием.

13. Для исключения несанкционированного доступа к информации, содержащей персональные данные, при покидании помещения необходимо запирать его на ключ.

V. Уборка помещений

14. Клининговая компания, оказывающая услуги по уборке помещений администрации города, должна предоставить в административно-хозяйственное подразделение список обслуживающего персонала.

15. Во время уборки в помещении должна быть приостановлена работа с персональными данными, должны быть выключены все компьютеры, на которых хранятся персональные данные, носители, содержащие персональные данные должны быть убраны в сейф.

VI. Требования по техническому укреплению

16. Ответственный за обеспечение безопасности персональных данных или начальник органа администрации города обеспечивает обязательное выполнение мероприятий по техническому укреплению и оборудованию специальными техническими средствами охраны, системами пожарной безопасности и должны руководствоваться следующими основными требованиями:

1) двери и окна должны иметь прочные и надежные петли, задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек;

2) конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол. Стекла в рамах должны быть надежно закреплены в пазах. На окнах первого этажа, а также верхних этажей – при возможности прямого просмотра помещения с улицы, должны быть установлены жалюзи.

Инструкция пользователей информационной системы персональных данных
в администрации города Магнитогорска

I. Общие положения

1. Настоящая инструкция определяет задачи, функции, обязанности, права и ответственность пользователей информационной системы персональных данных в администрации города.

2. Пользователи получают доступ к работам в информационной системе персональных данных только на основании утвержденного списка допущенных лиц.

3. В пределах своих должностных обязанностей пользователи обеспечивают безопасность персональных данных, обрабатываемых в информационной системе персональных данных.

II. Обязанности пользователей информационной системы
персональных данных

4. Хранить в тайне персональные данные, ставшие известными ему в соответствии с характером работы.

5. Хранить в тайне идентификаторы и пароли, используемые для входа в систему.

6. При обработке персональных данных руководствоваться правилами работы с общесистемным и прикладным программным обеспечением (ОС Windows, Microsoft Word, Microsoft Excel, и т.д.), средствами защиты информации.

7. Для хранения персональных данных использовать только учтенные установленным порядком машинные носители информации.

8. Соблюдать порядок учета, обращения и хранения зарегистрированных машинных носителей информации, отражая выдачу и приём машинных носителей информации «Журнале учета стационарных машинных носителей информации» и «Журнале учёта съемных машинных носителей информации».

9. Покидая рабочее место, выключать или блокировать персональную электронно-вычислительную машину. Не допускать бесконтрольное присутствие посторонних лиц в помещении, где ведется обработка персональных данных.

10. Не допускать посторонних лиц к техническим средствам.

11. Использовать только штатные программные и технические средства. Установка новых программных и технических средств, должна согласовываться с администратором по техническому обеспечению безопасности персональных данных, системным администратором.

12. Производить выключение питания ПЭВМ, после завершения своей работы при помощи стандартной процедуры операционной системы.

III. Пользователям информационной системы персональных данных запрещается

13. Использовать нештатные технические средства и системы; самостоятельно вносить изменения в состав, конфигурацию, и размещение основных технических средств.

14. Использовать нештатные программные средства; самостоятельно вносить изменения в их состав.

15. Проводить обработку персональных данных при неисправно работающих средствах защиты информации.

16. Вносить изменения в средства защиты информации, используемые в информационной системе персональных данных.

17. Производить копирование персональных данных на неучтенные машинные носители информации.

18. Допускать к работам в информационные системы персональных данных работников, не включенных в перечень работников, обработка персональных данных которым необходима в связи с исполнением служебных обязанностей.

19. Обрабатывать персональные данные в случае, если требования и предписания на обработку персональных данных не соблюдаются, имеют место неисправности, создающие предпосылки для утечки персональных данных.

IV. Права пользователей информационной системы персональных данных

20. Обрабатывать персональные данные в соответствии с должностными обязанностями.

21. Обращаться к администратору информационной системы персональных данных.

V. Ответственность пользователей информационной системы персональных данных

22. Пользователи информационной систем персональных данных несут персональную ответственность в соответствии с действующим законодательством за разглашение персональных данных, утрату учтенных машинных носителей информации и организационно-распорядительных документов.

Инструкция
администратора по техническому обеспечению безопасности персональных
данных в администрации города Магнитогорска

I. Общие положения

1. Данная инструкция определяет основные обязанности, права, и ответственность администратора по техническому обеспечению безопасности персональных данных в администрации города (далее – администратор).
2. Администратор является штатным сотрудником органа администрации города.
3. Администратор назначается распоряжением администрации города.
4. В прямые служебные обязанности администратора входит контроль выполнения требований и организационных мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных дополнительно к своим непосредственным обязанностям.

II. Обязанности администратора

5. Анализировать журналы обращений к информационным системам персональных данных и регистрации системных событий.
6. Осуществлять настройку, администрирования и контроль антивирусного программного обеспечения, регулярно обновлять антивирусные базы и проводить проверки согласно инструкциям.
7. Осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных.
8. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования информационной системы персональных данных и осуществления несанкционированного доступа к персональным данным и техническим средствам вычислительной техники. При выявлении таковых сообщать о них ответственному за обеспечение безопасности персональных данных в администрации города.

III. Права администратора

9. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций по защите информации, регламентирующих порядок действий по защите информации.
10. Обеспечивать установку, настройку и своевременное обновление элементов информационной системы персональных данных:
 - 1) программного обеспечения автоматизированных рабочих мест и серверов (операционные системы, прикладное и специальное ПО);
 - 2) аппаратных средств;

3) аппаратных и программных средств защиты.

11. Обеспечивать работоспособность элементов информационной системы персональных данных и локальной вычислительной сети.

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

13. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

14. В случае отказа работоспособности технических средств и программного обеспечения элементов информационной системы персональных данных, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

15. Проводить периодический контроль принятых мер по защите, в пределах возложенных на него функций.

16. Информировать ответственного за обеспечение защиты персональных данных в администрации города о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам информационной системы персональных данных.

17. Присутствовать при выполнении технического обслуживания элементов информационной системы персональных данных, сторонними физическими людьми и организациями.

18. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

19. Требовать от пользователей информационной системы персональных данных соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности персональных данных в информационной системе персональных данных.

20. Обращаться к ответственному за обеспечение безопасности персональных данных в администрации города с требованием прекращения работы информационной системе персональных данных при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности

IV. Ответственность администратора

21. На администратора возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации.

22. Администратор несет ответственность согласно действующему законодательству за разглашение сведений ограниченного распространения, ставших известными ему в период исполнения должностных обязанностей.

Инструкция
по резервному копированию и восстановлению информационных ресурсов
в администрации города Магнитогорска

I. Общие положения

1. Настоящая инструкция разработана с целью определения порядка резервирования данных для последующего восстановления работоспособности информационной системы персональных данных в администрации города при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.).

2. Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных.

II. Способы, средства и системы резервирования

3. Резервное копирование (архивация) информации обеспечивается специализированными программными средствами, позволяющими обеспечивать сохранность обрабатываемой информации в случае ее утери или повреждения.

4. Резервные копии рекомендуется хранить на отчуждаемых носителях информации в сейфе, с соответствующим отражением в «Журнале учета съемных машинных носителей информации», либо на жёстких дисках автоматизированной системы, на логическом диске отличном от системного, в директории с разграничением доступа только для администратора.

III. Резервируемое общесистемное и специальное программное обеспечение,
программное обеспечение средств защиты информации,
базы персональных данных

5. Для резервирования следует выбирать следующие объекты:

1) электронные документы, содержащие персональные данные, хранящиеся на жестких дисках компьютеров информационной системы персональных данных, в том числе баз данных;

2) копии прикладного программного обеспечения, используемого для обработки персональных данных;

3) информацию пользователей, необходимую для работы с персональными данными.

IV. Порядок резервирования и хранения резервных копий,
периодичность резервирования

6. Резервное копирование информации, хранящейся в базе данных программного обеспечения настраивается и производится под контролем ответственного за обеспечение безопасности персональных данных однократно

после подготовки информационной системы персональных данных Организации к работе и хранится:

- 1) одна копия – на жестком диске сервера баз данных;
- 2) вторая копия – на отчуждаемом учетном носителе.

7. Резервное копирование пользовательской информации производится еженедельно администратором.

8. Сохранять полученный образ необходимо на диске, отличном от архивируемого.

9. После окончания процесса резервного копирования полученный полный образ диска следует скопировать на отчуждаемый учетный носитель.

10. При втором и последующих резервных копированиях текущего месяца возможно создание инкрементного образа.

11. В случае нехватки свободного дискового пространства для сохранения файла образа следует удалить наиболее старый архивный образ. Удалять следует полный образ и одновременно соответствующие ему инкрементные образы.

12. На диске ПЭВМ должны храниться одновременно полный образ и (при наличии) соответствующие ему инкрементные образы не менее чем за два месяца: текущий и предыдущий.

V. Порядок восстановления повреждённых или уничтоженных документов конфиденциальной информации

13. В случае необходимости восстановления данных из резервной копии, для восстановления следует использовать наиболее поздний архивный образ. В случае невозможности использования наиболее позднего образа по каким-либо причинам образ, используемый для восстановления, выбирается совместным решением пользователя, администратора и ответственного за обеспечение безопасности персональных данных.

Инструкция об особенностях обработки персональных данных,
осуществляемой без использования средств автоматизации
в администрации города Магнитогорска

I. Общие положения

1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее – персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

3. Правила обработки персональных данных, осуществляемой без использования средств автоматизации установлены в соответствии с Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

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

4. Персональные данные 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).

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

6. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (работники администрации города – оператор или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых

персональных данных, а также об особенностях и правилах осуществления такой обработки.

7. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

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

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

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

9. Правила, предусмотренные настоящей инструкцией, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

10. Уточнение персональных данных 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 носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

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

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

12. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

13. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Правила
осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных
в администрации города Магнитогорска

1. Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации города организовывается проведение плановых и внеплановых проверок условий обработки персональных данных на предмет соответствия Федеральному закону «О персональных данных», принятым в соответствии с ним нормативным правовым актам и локальным актом администрации города (далее – проверки).

3. Проверки проводятся в администрации города на основании ежегодного плана или на основании поступившего в администрацию города письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

Ежегодный план проверок разрабатывается и утверждается постоянно действующей технической комиссией по технической защите информации для осуществления внутреннего контроля соответствия обработки персональных данных требованиям, предусмотренным Федеральным законом «О персональных данных» (далее – Комиссия).

4. В плане по каждой проверке устанавливается объект внутреннего контроля, проверяемый период, срок проведения проверки, ответственные исполнители.

5. Основанием для проведения внеплановой проверки является поступившее в администрацию города письменное обращение субъекта персональных данных или его представителя о нарушении правил обработки персональных данных.

6. Проведение внеплановой проверки организуется в течение 5 рабочих дней с даты поступления обращения.

7. Срок проведения проверки не может превышать месяц со дня принятия решения о ее проведении.

8. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность персональных данных субъектов персональных данных, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных.

9. По результатам каждой проверки Комиссией проводится заседание. Решения, принятые на заседаниях Комиссии, оформляются протоколом.

10. По существу поставленных в обращении (жалобе) вопросов Комиссия в течение 5 рабочих дней со дня окончания проверки направляет письменный ответ заявителю.

Инструкция
по организации парольной защиты и защиты от несанкционированного доступа
на объектах информатизации в администрации города Магнитогорска

I. Основные положения

1. Данная инструкция регламентирует организационно - техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в органах администрации города, а также контроль за действиями пользователей автоматизированных рабочих мест, на которых обрабатываются персональные данные, при работе с паролями.
2. Ответственность и контроль за действиями пользователей автоматизированных рабочих мест, на которых обрабатываются персональные данные, возлагается на ответственного за обеспечение безопасности персональных данных в органе администрации города.

II. Правила формирования паролей

3. Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:
 - 1) длина пароля должна быть не менее 8 символов;
 - 2) в числе символов пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
 - 3) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;
 - 4) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях;
 - 5) личный пароль пользователь не имеет права сообщать никому.
4. Пароли хранятся в запечатанном конверте и передаются на хранение ответственному за обеспечение безопасности персональных данных в органе администрации города.
5. Опечатанные конверты с паролями должны храниться в сейфе или шкафу, запираемом на ключ.

III. Ввод пароля

6. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или

в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

IV. Порядок смены личных паролей

7. Смена паролей должна проводиться регулярно, не реже одного раза в квартал.

8. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

9. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за обеспечение безопасности персональных данных, администратора органа администрации города и других сотрудников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

10. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 7 настоящей инструкции.

V. Хранение пароля

11. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

12. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6. Действия в случае утери и компрометации пароля

13. В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 9 или п. 10 настоящей инструкции в зависимости от полномочий владельца скомпрометированного пароля.

Инструкция
по организации антивирусной защиты в администрации города

I. Общие положения

1. Данная инструкция определяет требования к организации защиты персональных данных в администрации города от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность работников администрации города за их выполнение.

2. К использованию в администрации города допускаются только лицензионные и сертифицированные средства антивирусной защиты, централизованно закупленные у разработчиков или поставщиков данных средств.

3. Установка средств антивирусного контроля на компьютерах (серверах локальной вычислительной сети органа администрации города) осуществляется администратором по техническому обеспечению персональных данных (далее – администратор), настройка параметров средств антивирусного контроля осуществляется в соответствии с эксплуатационной документацией на антивирусные средства.

II. Применение средств антивирусного контроля.

4. Ежедневно в начале работы при загрузке компьютера (для серверов локальной вычислительной сети – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов автоматизированных рабочих мест (далее – АРМ).

5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием, отправкой или записью на съемный носитель.

6. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено ответственным за обеспечение безопасности персональных данных в органе администрации города на предмет отсутствия вредоносного программного обеспечения. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка:

- на защищаемых серверах и АРМ – администратором органа администрации города;

- на других серверах и АРМ, не требующих защиты, – лицом, установившим (изменившим) программное обеспечение, в присутствии и под контролем начальника отдела информационно-правового обеспечения органа администрации города или сотрудника, им уполномоченного.

8. При возникновении подозрения на наличие вредоносного ПО (ошибки в работе программ, появление графических и звуковых эффектов, искажения данных, пропадание файлов, частое появление сообщений о системных ошибках, замедление работы компьютера и т.п.) сотрудник органа администрации города самостоятельно или вместе с администратором органа администрации города должен провести внеочередной антивирусный контроль своего АРМ. При необходимости привлечь ответственного за обеспечение безопасности персональных данных органа администрации города для определения им факта наличия или отсутствия вредоносного ПО.

9. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники органа администрации города обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов начальника и администратора органа администрации города, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора органа администрации города).

III. Обязанности

10. Обязанность за организацию антивирусного контроля в органе администрации города в соответствии с требованиями настоящей Инструкции возлагается на ответственного за обеспечение безопасности персональных данных в органе администрации города.

11. Обязанность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на администратора органа администрации города и всех сотрудников органа администрации города, являющихся пользователями автоматизированных рабочих мест администрации.

12. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, проверка работоспособности программы) органа администрации города, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками органа администрации города осуществляется администратором органа администрации города.

Приложение № 29
к распоряжению
администрации города
от 29.08.2021 № 341-р

«наименование органа администрации»
администрации города Магнитогорска Челябинской области

Журнал учета выявленных инцидентов информационной безопасности

Начато:	
Окончено:	
Количество листов:	
Срок хранения:	5 лет

Приложение № 30
к распоряжению
администрации города
от 10.08.2021 № 241-р

«наименование органа администрации»
администрации города Магнитогорска Челябинской области

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

Начато:	
Окончено:	
Количество листов:	
Срок хранения:	5 лет

**Журнал по землярному учету средств криптографической защиты информации,
технической и эксплуатационной документации к ним**