КАЛУГАИНФОРМТЕХ

Государственное бюджетное учреждение
Калужской области
«Агентство информационных технологий
Калужской области»

(ГБУ КО «Калугаинформтех»)

П Р И К А З

от «20» октября 2023 г. **№ 43**

Об утверждении правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом «О персональных данных»

В соответствии с Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» **ПРИКАЗЫВАЮ:**

1. Утвердить правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами в ГБУ КО «Калугаинформтех» (приложение № 1).
2. Утвердить план проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом «О персональных данных» (приложение № 2).
3. Приказы ГБУ КО «Калугаинформтех» от 24.02.2015 № 11, от 15.04.2015 № 18 признать утратившими силу.
4. Главному специалисту отдела ОПиКО Альминайте Я.С. ознакомить заинтересованных сотрудников учреждения с настоящим приказом.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Директор **А.С. Корабанов**

ПРИЛОЖЕНИЕ № 1
к приказу
ГБУ КО «Калугаинформтех»
от 20 октября 2023 г. № 43

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и приказами ГБУ КО «Калугаинформтех»

1. Общие положения

1.1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и приказами ГБУ КО «Калугаинформтех» (далее – Правила) разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими действующими нормативно-правовыми актами по защите персональных данных.

1.2. Настоящие Правила определяют цели, сроки и порядок осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям (далее – внутренний контроль) в ГБУ КО «Калугаинформтех».

2. Цели внутреннего контроля

2.1. Внутренний контроль в ГБУ КО «Калугаинформтех» производится в целях:

1) проверки соблюдения сотрудниками ГБУ КО «Калугаинформтех», непосредственно осуществляющими обработку персональных данных, требований Федерального закона «О персональных данных», принятых в соответствии с ним нормативных правовых актов и приказов ГБУ КО «Калугаинформтех»;

2) предотвращения нарушений, связанных с обработкой и защитой персональных данных в ГБУ КО «Калугаинформтех»;

3) совершенствования системы защиты персональных данных в ГБУ КО «Калугаинформтех».

3. Организация внутреннего контроля

3.1. Внутренний контроль соответствия обработки персональных данных установленным требованиям в ГБУ КО «Калугаинформтех» осуществляется путём проведения периодических проверок условий обработки персональных данных в подразделениях ГБУ КО «Калугаинформтех», обрабатывающих персональные данные.

3.2. Плановые внутренние проверки проводит сотрудник, ответственный за организацию обработки персональных данных, внеплановые внутренние проверки проводит комиссия по организации обработки и защиты персональных данных в ГБУ КО «Калугаинформтех».

3.3. Комиссия по организации обработки и защиты персональных данных в ГБУ КО «Калугаинформтех» утверждается приказом директора учреждения. В состав комиссии не может входить сотрудник, прямо или косвенно заинтересованный в ее результате.

3.4. Сроки и периодичность проведения плановых внутренних проверок в ГБУ КО «Калугаинформтех» определяются планом осуществления внутренних проверок соответствия обработки персональных данных установленным требованиям, утверждаемым приказом директора учреждения.

3.5. Основания для проведения внеплановых проверок:

3.5.1. решение руководителя ГБУ КО «Калугаинформтех» (далее – руководитель);

3.5.2. выявление ответственными сотрудниками нарушений правил обработки персональных данных в ГБУ КО «Калугаинформтех», которые могут нанести существенный вред субъекту персональных данных, установленных протоколом проведения внутренней проверки, утвержденным руководителем;

3.5.3. письменное заявление субъекта персональных данных о нарушении его прав.

3.6. Проведение внеплановой внутренней проверки организуется в течение трех рабочих дней с момента наступления событий, указанных в пункте 3.5. настоящих Правил.

3.7. Сотрудники, осуществляющие проверку (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.

4. Порядок проведения внутренних проверок

4.1. Внутренняя проверка условий обработки персональных данных в ГБУ КО «Калугаинформтех» осуществляется непосредственно на месте обработки персональных данных способом опроса и осмотра рабочих мест сотрудников ГБУ КО «Калугаинформтех», осуществляющих обработку персональных данных.

4.2. В ходе проведения внутренней проверки проверяется:

4.2.1. наличие и актуальность документации, связанной с обработкой персональных данных;

4.2.2. выполнение требований Федерального закона «О персональных данных», принятых в соответствии с ним нормативных правовых актов и приказов ГБУ КО «Калугаинформтех», в том числе:

- правил обработки персональных данных в ГБУ КО «Калугаинформтех»;
- правил рассмотрения запросов субъектов персональных данных или их представителей в ГБУ КО «Калугаинформтех»;
- порядка доступа сотрудников ГБУ КО «Калугаинформтех» в помещения, в которых ведется обработка персональных данных;

4.2.3. отсутствие нарушений порядка обработки и защиты персональных данных;

4.2.4. соблюдение пользователями информационных систем персональных данных порядка работы со средствами защиты информации;

4.2.5. соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями информации;

4.2.6. соблюдение порядка резервирования информации и хранения резервных копий.

4.3. Плановая внутренняя проверка проводиться согласно утвержденного плана. Внеплановая внутренняя проверка должна быть завершена не позднее чем через месяц со дня принятия решения о ее проведении.

5. Порядок оформления результатов внутренних проверок

5.1. Ежеквартально должностное лицо, проводившее плановую внутреннюю проверку, составляют протокол по форме, приведенной в приложении к настоящим Правилам.

При проведения внеплановой внутренней проверки не позднее месяца со дня принятия решения о ее проведении комиссия подготавливает протокол по форме, приведенной в приложении к настоящим Правилам.

В случае проведения внеплановой внутренней проверки в соответствии с пунктом 3.5.3. комиссия в течении 5 рабочих дней со дня окончания проверки дает письменный ответ субъекту персональных данных (заявителю) о результатах проверки.

5.2. Выявленные нарушения соответствия обработки персональных данных установленным требованиям фиксируются в протоколе, а также делается запись о планируемых мероприятиях по устранению нарушений и сроках их исполнения.

5.3. Сотрудник, ответственный за организацию обработки персональных данных либо председатель комиссии, проводившие внутреннюю проверку, докладывают руководителю о результатах её проведения и мерах, необходимых для устранения нарушений и представляют на утверждение протокол проведения внутренней проверки.

Приложение к Правилам
осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных,
установленным Федеральным законом
«О персональных данных», принятыми в соответствии
с ним нормативными правовыми актами
и приказами ГБУ КО «Калугаинформтех»

УТВЕРЖДАЮ
Руководитель ГБУ КО «Калугаинформтех»
_____ Ф.И.О.
«____» _____ 20 ___ г.

Протокол № ____
проведения внутренней проверки соответствия обработки персональных данных установленным требованиям в ГБУ КО «Калугаинформтех»

Настоящий Протокол составлен о том, что «___». _____20___ г.

_____

_____

(указывается ФИО и должность сотрудника, проводившего проверку либо наименование комиссии)

_____

_____

произведена внутренняя проверка соответствия обработки персональных данных требованиям, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и приказами ГБУ КО «Калугаинформтех»

_____

_____

(наименование подразделения ГБУ КО «Калугаинформтех», информационной системы персональных данных)

_____

_____

При проведении внутренней проверки проверено:

_____

_____

_____

_____

Выявленные нарушения:

_____

_____

_____

_____

Меры по устранению нарушений:

_____

_____
_____
_____
_____

Срок устранения нарушений: _____

Лицо, ответственное
за организацию обработки персональных данных

Должность _____ Ф.И.О.

либо

Комиссия в составе:

Председатель _____ Ф.И.О.

Члены комиссии

_____ Ф.И.О.
_____ Ф.И.О.

ПРИЛОЖЕНИЕ № 2
к приказу ГБУ КО «Калугаинформтех»
от 20 октября 2023 г. № 43

План проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом «О персональных данных»

Мероприятие	Периодичность	Исполнитель
Контроль над соблюдением режима обработки персональных данных (далее – ПДн)	постоянно	сотрудник, ответственный за организацию обработки персональных данных
Контроль над соблюдением режима защиты ПДн	постоянно	сотрудник, ответственный за организацию обработки персональных данных
Контроль над выполнением антивирусной защиты	постоянно	сотрудник, ответственный за организацию обработки персональных данных
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	постоянно	сотрудник, ответственный за организацию обработки персональных данных
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах информационных систем персональных данных (далее – ИСПДн)	постоянно	сотрудник, ответственный за организацию обработки персональных данных совместно с начальником отдела сопровождения средств ИКТ
Контроль соблюдения пользователями ИСПДн порядка работы со средствами защиты информации	Ежемесячно	сотрудник, ответственный за организацию обработки персональных данных совместно с начальником отдела сопровождения средств ИКТ
Контроль за обеспечением резервного копирования	Ежемесячно	сотрудник, ответственный за организацию обработки персональных данных совместно с начальником отдела сопровождения средств ИКТ

Поддержание в актуальном состоянии нормативно-организационных документов распорядительных и нормативно-методических документов, регламентирующих обработку персональных данных	Ежемесячно	сотрудник, ответственный за организацию обработки персональных данных
Проверка порядка использования технических средств защиты ПДн	Ежемесячно	сотрудник, ответственный за организацию обработки персональных данных совместно с начальником отдела сопровождения средств ИКТ
Контроль выполнения требований по режиму доступа в здание, защищаемые помещения и на автоматизированные рабочие места, обрабатывающие ПДн	Ежемесячно	сотрудник, ответственный за организацию обработки персональных данных
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	сотрудник, ответственный за организацию обработки персональных данных
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, прогнозирование появления новых, еще неизвестных, угроз	Ежегодно	сотрудник, ответственный за организацию обработки персональных данных совместно с начальником отдела сопровождения средств ИКТ
Составление акта проверки	Ежеквартально	сотрудник, ответственный за организацию обработки персональных данных