Муниципальное Бюджетное Учреждение «Дом ученых»

(МБУ «Дом учёных»)

УТВЕРЖДАЮ
Директор МБУ «Дом ученых»

И.В.Мидюков

14.08.2024 г.

ПОЛОЖЕНИЕ

о защите персональных данных

г.Обнинск

1. Общие положения

1.1. Положение о защите персональных данных МБУ «Дом ученых» (далее также— Работодатель) разработано в соответствии с Трудовым кодексом РФ, Федеральным законом от 27.07.2006 № 152-ФЗ, нормативными правовыми актами в области защиты персональных данных, действующими на территории России (далее — Положение).

1.2. Цель настоящего Положения – защита персональных данных работников МБУ «Дом ученых» от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

1.3. В целях настоящего Положения:

- под персональными данными (далее – ПД) понимается любая информация, прямо или косвенно относящаяся к субъекту персональных данных;
- под угрозами безопасности ПД понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;
- под уровнем защищенности ПД понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПД при их обработке в информационной системе.

1.4. Настоящее Положение распространяется на работников МБУ «Дом ученых». Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

1.5. Настоящее Положение вступает в силу со дня его утверждения директором МБУ «Дом ученых» и действует бессрочно до принятия нового положения.

2. Защита персональных данных

2.1. Работодатель принимает следующие меры по защите ПД:

2.1.1. Назначение лица, ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите ПД.

2.1.2. Установление правил доступа к ПД, обеспечение регистрации и учета всех действий, совершаемых с ПД.

2.1.3. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их трудовыми обязанностями.

2.1.4. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

2.1.5. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

2.1.6. Соблюдение условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ.

2.1.7. Обнаружение фактов несанкционированного доступа к ПД.

2.1.8. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.1.9. Обучение работников, непосредственно осуществляющих обработку ПД, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Работодателя в отношении обработки ПД, локальным актам по вопросам обработки персональных данных.

2.1.10. Осуществление внутреннего контроля и аудита.

Внутренние плановые проверки осуществляются на основании ежегодного плана, который утверждается директором МБУ «Дом ученых». Внутренние внеплановые проверки осуществляются по решению работника, ответственного за организацию обработки персональных данных. Основанием для них служит информация о нарушении законодательства в области персональных данных, поступившая в устном или письменном виде. По итогам внутренней проверки оформляется докладная записка на имя директора. Если выявлены нарушения, в документе приводится перечень мероприятий по их устранению и соответствующие сроки.

2.1.11. Определение типа угроз безопасности и уровней защищенности ПД, которые хранятся в информационных системах.

2.2. Угрозы защищенности персональных данных.

2.2.1. Угрозы первого типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных.

2.2.2. Угрозы второго типа. Потенциальные проблемы с прикладным программным обеспечением — внешними программами, которые установлены на компьютерах работников.

2.2.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

2.3. Уровни защищенности персональных данных.

2.3.1. Первый уровень защищенности. Если работодатель отнес информационную систему к первому типу угрозы или если тип угрозы второй, но работодатель обрабатывает специальные категории ПД более 100 тыс. физических лиц без учета работников.

2.3.2. Второй уровень защищенности. Если тип угрозы второй и работодатель обрабатывает биометрические и специальные категории ПД работников вне зависимости от их количества или специальные категории ПД менее чем 100 тыс. физических лиц, или любые другие категории ПД более чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

2.3.3. Третий уровень защищенности. Если при втором типе угрозы работодатель обрабатывает общие ПД работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории ПД работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает биометрические ПД, или при третьем типе угрозы работодатель обрабатывает общие ПД более чем 100 тыс. физических лиц.

2.3.4. Четвертый уровень защищенности. Если при третьем типе угрозы работодатель обрабатывает только общие ПД работников или менее чем 100 тыс. физических лиц.

2.4. При четвертом уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещаете информационную систему;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных к работе с ПД;
- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

2.5. При третьем уровне защищенности ПД дополнительно к мерам, перечисленным в пункте 2.4 настоящего Положения, работодатель назначает ответственного за обеспечение безопасности ПД в информационной системе.

2.6. При втором уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 2.4, 2.5 настоящего Положения, работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

2.7. При первом уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 2.4—2.6 настоящего Положения, работодатель:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к ПД в системе;
- создает отдел, ответственный за безопасность ПД в системе, либо возлагает такую обязанность на один из существующих отделов работодателя.

2.8. В целях защиты ПД на бумажных носителях работодатель:

- приказом назначает ответственного за обработку ПД;
- ограничивает допуск в помещения, где хранятся документы, которые содержат ПД работников;
- хранит документы, содержащие ПД работников, в шкафах, запирающихся на ключ;
- хранит трудовые книжки работников в сейфе в отделе кадров.

2.9. В целях обеспечения конфиденциальности документы, содержащие ПД работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии и службы охраны труда работодателя.

2.10. Работники отдела кадров, бухгалтерии и службы охраны труда работодателя, допущенные к ПД работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки ПД работников не допускаются.

2.11. Допуск к документам, содержащим ПД работников, внутри организации осуществляется на основании Регламента допуска работников к обработке персональных данных.

2.12. Передача ПД по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством РФ, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.13. Передача информации, содержащей сведения о ПД работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

3. Цели обработки персональных данных

3.1. Работодатель может обрабатывать персональные данные работников в следующих случаях:

3.1.1. от работника получено согласие на обработку его персональных данных;

3.1.2. работодатель выполняет обязанности, которые на него возложены законодательством Российской Федерации;

3.1.3. в связи с участием в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах, а также для исполнения судебного акта, акта другого органа или должностного лица в соответствии с законодательством Российской Федерации об исполнительном производстве;

3.1.4. для защиты жизни, здоровья или иных жизненно важных интересов работника, если невозможно получить его согласие.

3.2. Работодатель обрабатывает персональные данные в следующих целях:

3.2.1. Ведение кадрового и бухгалтерского учета.

В рамках указанной цели обрабатываются следующие ПД работников:

- фамилия, имя, отчество;
- дата, месяц, год рождения;
- семейное положение;
- пол;
- гражданство;
- адрес регистрации и места жительства;
- данные документа, удостоверяющего личность;
- СНИЛС;
- ИНН;
- доходы;
- номер расчетного счета;
- реквизиты банковской карты;
- номер лицевого счета;
- профессия, должность;
- сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации).

Обрабатываемые в рамках указанной цели ПД не относятся к специальным категориям или биометрическим.

ПД обрабатываются с использованием средств автоматизации и без использования таких средств.

ПД обрабатываются в период действия трудового договора с работником. Документы с ПД хранятся в течение срока, установленного законодательством РФ. Срок хранения ПД в информационных системах соответствует сроку хранения аналогичных бумажных документов с ПД.

Персональные данные подлежат уничтожению по окончании срока хранения документов, которые содержат ПД, в порядке, предусмотренном настоящим Положением.

3.2.2. Обеспечение соблюдения трудового законодательства.

В рамках указанной цели обрабатываются следующие ПД работников, не относящиеся к специальным категориям или биометрическим:

- фамилия, имя, отчество;
- дата, месяц, год рождения;
- семейное положение;
- пол;
- гражданство;
- адрес регистрации и места жительства;
- данные документа, удостоверяющего личность;
- адрес электронной почты;
- номер телефона;
- СНИЛС;
- ИНН;
- доходы;
- номер расчетного счета;
- реквизиты банковской карты;
- номер лицевого счета; данные водительского удостоверения;
- профессия;
- должность;
- сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации);
- отношение к воинской обязанности, сведения о воинском учете;
- сведения об образовании;
- сведения о состоянии здоровья.

В рамках указанной цели обрабатываются следующие ПД работников –специальные категории ПД: сведения о состоянии здоровья.

В рамках указанной цели могут обрабатываться следующие ПД родственников работников, не относящиеся к специальным категориям или биометрическим:

- фамилия, имя, отчество;
- дата, месяц, год рождения;
- семейное положение;
- адрес регистрации и места жительства;
- данные документа, удостоверяющего личность;
- адрес электронной почты;
- номер телефона;
- должность;
- сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования организации);
- отношение к воинской обязанности, сведения о воинском учете;
- сведения об образовании.

ПД обрабатываются с использованием средств автоматизации и без использования таких средств.

ПД обрабатываются в период действия трудового договора с работником. Документы с ПД хранятся в течение срока, установленного законодательством РФ. Срок хранения ПД в информационных системах соответствует сроку хранения аналогичных бумажных документов с ПД.

Персональные данные подлежат уничтожению по окончании срока хранения документов, которые содержат ПД, в порядке, предусмотренном настоящим Положением.

3.2.3. Обеспечение соблюдения налогового законодательства.

В рамках указанной цели обрабатываются следующие ПД работников:

- фамилия, имя, отчество;
- дата, месяц, год рождения;
- семейное положение;
- пол;
- гражданство;
- адрес регистрации и места жительства;
- данные документа, удостоверяющего личность;
- СНИЛС;
- ИНН;
- доходы;
- номер расчетного счета;
- реквизиты банковской карты;
- номер лицевого счета;
- должность;
- сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации).

Обрабатываемые в рамках указанной цели ПД не относятся к специальным категориям или биометрическим.

ПД обрабатываются с использованием средств автоматизации и без использования таких средств.

ПД обрабатываются в период действия трудового договора с работником. Документы с ПД хранятся в течение срока, установленного законодательством РФ. Срок хранения ПД в информационных системах соответствует сроку хранения аналогичных бумажных документов с ПД.

Персональные данные подлежат уничтожению по окончании срока хранения документов, которые содержат ПД, в порядке, предусмотренном настоящим Положением.

3.2.4. Обеспечение пропускного режима на территорию Работодателя.

В рамках указанной цели обрабатываются следующие ПД работников, не относящиеся к специальным категориям или биометрическим:

- фамилия, имя, отчество;
- дата, месяц, год рождения;
- адрес регистрации и места жительства;
- данные документа, удостоверяющего личность;
- номер телефона;
- данные водительского удостоверения.

В рамках указанной цели обрабатываются следующие ПД работников, относящиеся к биометрическим — данные изображения лица, полученные с помощью фотоустройств.

ПД обрабатываются с использованием средств автоматизации и без использования таких средств.

ПД обрабатываются в течение действия трудового договора с работником.

ПД подлежат уничтожению в течение 30 дней с момента увольнения работника в порядке, предусмотренном настоящим Положением.

3.2.5. Подбор персонала на вакантные должности.

В рамках указанной цели обрабатываются следующие ПД соискателей:

- фамилия, имя, отчество;
- дата, месяц, год рождения;
- гражданство;
- адрес регистрации;
- адрес электронной почты;
- номер телефона;
- профессия;
- должность;
- сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации);
- сведения об образовании.

Обрабатываемые в рамках указанной цели ПД не относятся к специальным категориям или биометрическим.

ПД обрабатываются с использованием средств автоматизации и без использования таких средств.

ПД обрабатываются в течение периода принятия решения о трудоустройстве.

ПД подлежат уничтожению в течение 30 дней с момента принятия решения о трудоустройстве в порядке, предусмотренном настоящим Положением.

4. Права и обязанности работников

4.1. Работники имеют право на:

- доступ к своим ПД, включая право на получение копий любой записи, содержащей ПД работника, за исключением случаев, предусмотренных федеральным законом;
- уточнение своих ПД, их блокирование или уничтожение в случае, если ПД являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отзыв согласия на обработку ПД. Для этого работник должен направить работодателю в письменной форме отзыв согласия. В случае отзыва согласия на обработку ПД Работодатель вправе продолжить обработку ПД без согласия Работника при наличии оснований, предусмотренных пунктами 3.1.2–3.1.4 настоящего Положения;
- требование прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных для распространения.

4.2. Работники обязаны:

- предоставлять Работодателю достоверные персональные данные;
- сообщать Работодателю об изменении своих персональных данных в течение 3 рабочих дней со дня наступления соответствующих изменений.

5. Обязанности Работодателя

5.1. Работодатель обязан:

- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении ПД;
- не сообщать ПД работников третьим лицам без письменного согласия работников, за исключением случаев, предусмотренных Трудовым кодексом или иными федеральными законами;
- разрешать доступ к ПД работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПД, которые необходимы для выполнения конкретных трудовых обязанностей.

6. Обязанности лиц, допущенных к обработке ПД

6.1. Работники, осуществляющие обработку ПД работников и контрагентов МБУ «Дом ученых», обязаны:

- не разглашать третьим лицам и работникам МБУ «Дом ученых» ПД, которые известны ему в связи с исполнением трудовых обязанностей;
- не использовать ПД с целью получения личной выгоды;

- выполнять требования законодательства РФ в области персональных данных и локальных нормативных актов МБУ «Дом ученых», регламентирующих порядок обработки персональных данных;
- докладывать своему непосредственному руководителю и директору МБУ «Дом ученых» обо всех фактах и попытках несанкционированного доступа к ПД и утечке персональных данных в соответствии с установленным в МБУ «Дом ученых» регламентом действий на случай такой утечки;
- после прекращения прав на допуск к персональным данным (перевод на другую должность, увольнение) не разглашать и не передавать ПД третьим лицам и не уполномоченным на это работникам МБУ «Дом ученых»;
- все материальные (бумажные и электронные) носители ПД при увольнении передать непосредственному руководителю.

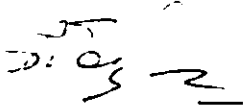
В случае разглашения ПД Работник может быть привлечен к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами. Кроме того, он может быть привлечен к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

7. Уничтожение персональных данных

7.1. Для уничтожения документов, которые содержат ПД, создается комиссия по уничтожению данных. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению

7.2. Бумажные носители информации уничтожаются с помощью шредера. Документом, подтверждающим уничтожение ПД, является акт об уничтожении персональных данных.

7.3. ПД, которые хранятся в информационных системах, удаляются из этих систем. Документом, подтверждающим удаление ПД, является акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных.

Специалист по кадрам  Н.Г. Горбачева