

«СОГЛАСОВАНО»

Председатель МОО-ПНО
ФГБНУ НЦПЗ

Шешенин В.С.

«29» июля 2022 г.

«УТВЕРЖДЕНО»

Приказом по ФГБНУ НЦПЗ
№ 97а от «29» июля 2022г.
Директор ФГБНУ НЦПЗ

Клюшник Т.П.

«29» июля 2022 г.

Дополнения
к Положению об обработке и защите персональных данных работников
Федерального государственного бюджетного научного учреждения
«Научный центр психического здоровья»
(ФГБНУ НЦПЗ)

Внести в Положение об обработке и защите персональных данных работников Федерального государственного бюджетного научного учреждения «Научный центр психического здоровья» (ФГБНУ НЦПЗ) следующие изменения:

1) Подраздел 2.3.3 подпункт «биометрические персональные данные» дополнить текстом следующего содержания:

Предоставление биометрических персональных данных не может быть обязательным, за исключением случаев, предусмотренных частью 2 статьи 11 Федерального закона от 27.07.2006г. №152-ФЗ.

2) Раздел 3 дополнить подразделами 3.2.4, 3.9 и 3.10 и текстом следующего содержания:

3.2.4. Работодатель вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом. В поручении оператора должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Федерального закона от 14.07.2022г. №266-ФЗ, обязанность по запросу оператора персональных данных в течение срока действия поручения оператора, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, обязанность обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона 14.07.2022г. №266-ФЗ, в том числе требование об уведомлении оператора о случаях, предусмотренных частью 3.1 статьи 21 Федерального закона 14.07.2022г. №266-ФЗ.

3.9. Работодатель определяет тип угроз безопасности и уровень защищенности персональных данных, которые хранятся в информационных системах, и предпринимает меры по защите информации:

3.9.1. При 4-м уровне защищенности персональных данных Работодатель:

- обеспечивает режим безопасности помещений, в которых размещается информационная система;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных до персональных данных;
- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

3.9.2. При 3-м уровне защищенности персональных данных, дополнительно к мерам, перечисленным в пункте 3.9.1 настоящего Положения, Работодатель назначает ответственного за обеспечение безопасности персональных данных в информационной системе.

3.9.3. При 2-м уровне защищенности персональных данных, дополнительно к мерам, перечисленным в пункте 3.9.1 и 3.9.2 настоящего Положения, Работодатель ограничивает доступ к электронному журналу сообщений, за исключением Работников, которым такие сведения необходимы для работы.

3.9.4. При 1-м уровне защищенности персональных данных, дополнительно к мерам, перечисленным в пункте 3.9.1 – 3.9.3 настоящего Положения, Работодатель:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к персональным данным в системе;
- создает отдел, ответственный за безопасность персональных данных в системе, либо возлагает такую ответственность на один из существующих отделов Работодателя.

3.10. Работодатель обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.