УТВЕРЖДАЮ
Генеральный директор
ООО «Глобал-М»
_____ М.Ш. Шихсаидов

09.01.2025

ПОЛОЖЕНИЕ
о защите персональных данных работников Общества с ограниченной ответственностью «Глобал-М» (ООО «Глобал-М»)
(новая редакция)

г.Махачкала – 2025

1. Общие положения

1.1. Положение о защите персональных данных ООО «Глобал-М» (далее – Работодатель) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ и иными нормативно-правовыми актами в области защиты персональных данных, действующими на территории России.

1.2. Цель настоящего Положения – защита персональных данных работников ООО «Глобал-М» 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 и изменения к нему утверждаются генеральным директором ООО «Глобал-М» и вводятся приказом. Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

1.5. Настоящее Положение вступает в силу с 09.01.2025 г.

2. Защита персональных данных

2.1. Работодатель принимает следующие меры по защите ПД:

- совершение всех операций по оформлению, ведению и хранению ПД только утвержденными работниками ООО «Глобус-М» в соответствии со своими обязанностями, определенными в должностных инструкциях,
- четкое распределение документов и информации между работниками,
- назначение лица, ответственного за обработку ПД, которое осуществляет организацию обработки ПД, внутренний контроль за соблюдением работниками требований к защите ПД,
- установление правил доступа к ПД, обеспечение регистрации и учета всех действий, совершаемых с ПД,
- установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями,

- сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами,
- соблюдение условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ,
- обнаружение фактов несанкционированного доступа к ПД,
- восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним,
- 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,
- осуществление внутреннего контроля и аудита,
- запрещена передача информации, содержащей сведения о ПД работников по телефону, факсу, электронной почте без письменного согласия работника.

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

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 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 до 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 и в сейфе в отделе бухгалтерии;
- хранит трудовые книжки работников в сейфе в кабинете юрисконсульта.

2.9. В целях обеспечения конфиденциальности документы, содержащие ПД работников, оформляются, ведутся и хранятся у сотрудников отвечающие за кадровый и бухгалтерский учет: юрисконсультом и работниками бухгалтерии работодателя.

2.10. Работники 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 **Приказа** 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.

2.14. Выдача ответов на письменные запросы других организаций и учреждений в пределах компетенций даются в письменной форме на бланке ООО «Глобал-М» и в объеме, позволяющем не разглашать излишние сведения о ПД работников.

2.15. Внешняя защита ПД работников осуществляется путем:

- определения порядка приема, учета и контроля посетителей,
- введение пропускного режима ООО «Глобал-М»,
- установка технических средств охраны, сигнализации, в частности, тревожной сигнализации (вызов наряда полиции по тревоге),
- охрана территории, зданий и помещений путем систем видеонаблюдения,
- выполнение требований по защите информации при интервьюировании и собеседовании.

3. Гарантии конфиденциальности персональных данных

3.1. Все работники организации ООО «Глобал-М», осуществляющие обработку ПД, обязаны хранить тайну о сведениях, содержащих ПД, в соответствии с Положением и требованиями законодательства РФ.

3.2. Работник вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

3.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством

Согласовано:

ФИО	должность	дата	подпись
Исмаилова Равиля Зинатулаевна	юрисконсульт	09.01.2025	

Прошито, пронумеровано и скреплено
печатью

количество листов 5

_____

«09» _____ 2025 г.