**Общество с ограниченной ответственностью**

**«Наше богатство»**

**(ООО «Наше богатство»)**

**ПРИКАЗ №\_\_\_\_**

г. Москва «\_\_\_» \_\_\_\_\_\_\_\_\_20\_\_ г.

**О назначении аудитора для проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных**

В целях обеспечения выполнения требований Федерального закона от 27.07.2006   
№ 152-ФЗ «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», главы 14 Трудового кодекса Российской Федерации и принятыми в соответствии с ними нормативными правовыми актами,

**ПРИКАЗЫВАЮ:**

1. Назначить генерального директора Иванова А.О. аудитором по проведению внутреннего контроля соответствия обработки персональных данных работников требованиям к защите персональных данных.

2. Установить периодичность проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных не реже чем один раз в год.

3. Установить срок проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных не более 7 рабочих дней.

4. Предоставлять результаты внутреннего контроля в виде протокола не позднее трех рабочих дней после завершения с указанием результатов оценки вреда, который может быть причинен субъектам персональных данных.

5. Ознакомить с настоящим приказом ответственного за организацию обработки персональных данных работников, руководителей структурных подразделений, лиц, допущенных к работе с персональными данными, а также лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения трудовых обязанностей.

6. Контроль исполнения настоящего приказа оставляю за собой.

Генеральный директор А.О.Иванов

**УТВЕРЖДАЮ**

Генеральный директор Общества с ограниченной ответственностью «Наше богатство»

\_\_\_\_\_\_\_\_\_\_А.О.Иванов

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

**ПРОТОКОЛ**

**внутреннего контроля соответствия обработки персональных данных в**

**ООО «Наше богатство»**

**требованиям к защите персональных данных работников**

1. Результаты рассмотрения вопросов по предметам контроля:

|  |  |  |
| --- | --- | --- |
| **Предмет контроля** | **Результат**  **рассмотрения** | **Степень возможного вреда субъектам персональных данных** |
| Документы, определяющие основания обработки персональных данных | Документы, регламентирующие порядок защиты, хранения, обработку и передачу персональных данных работников утверждены. На дату проверки актуальны. | **2** |
| Приказ о назначении ответственного лица за организацию обработки персональных данных работников | Приказом назначено ответственное лицо. Приказ актуален на дату проверки. | **1** |
| Представление актуальной информации в уполномоченный орган | Информация представлена в полном объеме | **2** |
| Соответствие установленных в перечне персональных данных категорий персональных данных фактически обрабатываемым | Установленные в положении категории соответствует фактически обрабатываемым. Обработки избыточных данных не выявлено. | **2** |
| Соответствие законных целей и оснований обработки всех категорий персональных данных | Цели и основания обработки соответствуют требованиям законов и иных нормативных правовых актов | **2** |
| Наличие утвержденного списка должностных лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими трудовых обязанностей | Список лиц утвержден приказом. Приказ актуален на дату проверки. | **2** |
| Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников | Право доступа лиц соответствует полномочиям, которые внесены в должностные инструкции. | **2** |
| Наличие обязательств о неразглашении персональных данных работников | Со всеми лицами, имеющими доступ к персональным данным, заключены обязательства о неразглашении | **2** |
| Перечень информационных систем эксплуатируемых при обработке персональных данных | Перечень утвержден приказом и актуален на дату проверки | **2** |
| Ознакомление работников с локальными актами в области обработки и обеспечения безопасности персональных данных | Все работники ознакомлены с локальными актами в области обработки персональных данных под роспись | **2** |
| Наличие в договорах с третьими лицами положений, касающихся обеспечения конфиденциальности и безопасности персональных данных | Договоры с третьими лицами содержат положения о конфиденциальности персональных данных | **1** |
| Проверка знаний у работников организационно распорядительных документов в области обработки и обеспечения безопасности персональных данных | Проверка знаний в области обеспечения безопасности персональных данных периодически проводиться с регистрацией в журнале | **2** |
| Доступ в здание, помещение | Порядок доступа в помещения с персональными данными утвержден приказом и соблюдается. Двери запираются на ключ. Утвержден список лиц, имеющих доступ в помещение | **2** |
| Перечень информационных систем персональных данных, эксплуатируемых в структурных подразделениях | Перечень информационных систем персональных данных необходимый для работы утвержден приказом | **1** |
| Мероприятия по уничтожению либо обезличиванию персональных данных, обрабатываемых, в связи с достижением целей обработки или утраты необходимости в достижении этих целей | Мероприятия проводятся своевременно экспертной комиссией и регистрацией Журнале | **1** |
| Условия хранения и состояние учета на бумажных носителях персональных данных | Приказом утвержден перечень мест хранения и требования. Требования соответствуют законодательству, условия соблюдаются. | **2** |
| Условия хранения и состояние учета машинных носителей персональных данных | Хранение машинных носителей персональных данных соответствует предъявляемым требованиям | **2** |
| Порядок и условия применения средств защиты информации при наличии таковых | Требования антивирусной защиты соблюдаются. Проводится проверка корректности расположения мониторов, исключающее несанкционированный просмотр экранов. Проводится выборочная проверка на предмет наличия возможных вредоносных программ и запрещенных информационных ресурсов. | **2** |
| Соблюдение требований к паролям доступа | Требования к паролям доступа соблюдаются | **1** |
| Размещение персональных данных работников в закрепленных за структурными подразделениями разделах официального сайта | Неправомерное размещенных персональных данных граждан на официальном сайте не выявлено | **1** |

2. Результат проверки: **нарушений не выявлено**.

3. Результат оценки вреда, который может быть причинен субъектам персональных данных (работники, их родственники, соискатели, клиенты, посетители, руководящий состав):

Установлена итоговая категория тяжести 2. Не требуются дополнительные действия, поскольку Работодатель периодически проводит мероприятия, которые позволяют убедиться, что соблюдения обязательных требований поддерживаются в рабочем состоянии. Необходимо дальнейшее поддержание соблюдения обязательных требований в рабочем состоянии, проведение мониторинга.

Аудитор \_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Подпись ФИО