

**Методические рекомендации
по обработке письменных запросов о предоставлении информации**

Данные методические рекомендации применяются при рассмотрении любых руководящих указаний и запросов о предоставлении сведений, в том числе содержащих персональные данные, и распространяются на органы государственной власти Кемеровской области - Кузбасса, иные государственные органы Кемеровской области - Кузбасса, органы местного самоуправления и подведомственные им учреждения.

При обработке поступивших запросов о предоставлении таких сведений ответственный специалист обязан произвести следующие действия:

1. убедиться в достоверности источника, запрашивающего информацию (доверенными источниками могут быть государственные информационные системы «Электронный документооборот Правительства Кемеровской области – Кузбасса», «Единая почтовая система Правительства Кемеровской области – Кузбасса», информационная система межведомственного электронного документооборота);

2. проверить, соблюдены ли требования по оформлению документа, такие как: оформление запроса на официальном бланке организации, наличие контактных данных исполнителя, регистрационного номера и даты документа;

3. связаться с органом (организацией), направившим запрос, для подтверждения подлинности запроса, при наличии любых подозрений на нелегитимность запроса.

4. уделить особое внимание документам, подписанным собственноручно, не электронной подписью, по возможности убедиться в подлинности подписи (документы, подписанные факсимильной подписью, к рассмотрению не подлежат);

5. не принимать к рассмотрению запросы, пришедшие с адресов электронной почты зарубежных производителей, например: gmail и иные;

6. передавать сведения, содержащие персональные данные, строго в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

7. применять СКЗИ сертифицированные ФСБ России, при передаче сведений с использованием сети «Интернет»;

8. особое внимание обращать на запросы от контролирующих органов (таких как УФСБ России, ФСТЭК России), содержащих запрос или требование о предоставлении информации, в том числе сведений о сотрудниках, содержащих персональные данные. При поступлении таких подозрительных запросов обязательно обратиться по контактным телефонам данного контролирующего органа для подтверждения легитимности запроса!

Кроме того, во всех перечисленных выше случаях необходимо проинформировать руководителя организации, юриста и ответственного за информационную безопасность.