Answer1: Responsible AI is the practice of designing, developing, and deploying AI with good intention to empower employees and businesses, and fairly impact customers and society—allowing companies to engender trust and scale AI with confidence.

Answer 2: Amazon started building machine learning programs in 2014 to review job applicants’ resumes. However, the AI-based experimental hiring tool had a major flaw: it was biased against women.

The model was trained to assess applications by studying resumes submitted to the company over a span of 10 years. As most of these resumes were submitted by men, the system taught itself to favor male candidates. This meant that the AI downgraded resumes with words such as “women’s” (as in the case with “women’s chess club captain”). Similarly, graduates from two all-women’s colleges were also ranked lower.

By 2015, the company recognized the tool was not evaluating applicants for various roles in a gender-neutral way, and the program was eventually disbanded. The incident came to light in 2018 after Reuters reported it.

Answer 3:Consequences of failing to comply with GDPR and the effect that could have on an organisation.

**Financial penalties**

Under GDPR, organisations who fail to comply and/or suffer a data breach could face a fine. In the most serious cases, this fine could be up to 17 million euros, or 4% of a company’s annual turnover. This upper limit far exceeds the current maximum fine of £500,000 allowed under the Data Protection Act.

When deciding whether to impose a fine following a data breach, the ICO will consider (amongst other things) the following:

1. The severity and duration of the data breach
2. Whether the breach was intentional or negligent
3. If the company has had a previous data breach
4. The type of personal data involved in the breach
5. Whether the breach affects the rights and freedoms of the individuals affected

**Damaged reputation**

More than either of the above consequences, perhaps the biggest ramification of failing to comply with GDPR is the damage to your company reputation, which can sometimes be beyond repair.

**Compensation for damages**

Under GDPR, individuals also have the right to claim compensation for any material and/or non-material damages which result from an infringement of the regulation. The most serious data breaches could result in a high volume of claims, which can be incredibly costly. Far better to have water-tight data protection procedures in place than experience a breach and face paying thousands -or millions- to affected customers further down the line.

While there are a number of implications associated with failing to comply with GDPR, the above are perhaps the most significant.

Answer 4: Spread the word throughout the organisation that GDPR compliance is a company-wide responsibility and that every team can help you achieve compliance. Arrange data protection training for any staff who are involved in data handling, or even any other teams that would benefit. The more you invest -not just financially but in terms of time and effort- in GDPR-compliance, the more your company will reap the rewards.