1. Responsible AI refers to the ethical and transparent use of artificial intelligence in decision-making processes. This includes ensuring that the algorithms used are fair, unbiased, and transparent in their decision-making, and that the data used to train and operate these algorithms is properly collected, stored, and processed in accordance with privacy laws and regulations. Additionally, responsible AI requires organizations to have strong governance and accountability frameworks in place, and to be transparent about the decisions made by their algorithms and how these decisions are arrived at.
2. There have been numerous instances where AI has failed or been used maliciously or incorrectly, including:

* Bias in facial recognition systems: In 2020, it was reported that facial recognition systems were biased against people with dark skin tones and women, leading to inaccurate identification and false arrests. (https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/)
* Predictive policing algorithms: Predictive policing algorithms, which use historical crime data to predict where crimes are likely to occur, have been criticized for perpetuating racial and socioeconomic biases, as well as for leading to over-policing in certain communities. (technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/)
* Algorithmic bias in hiring and lending: AI algorithms used in hiring and lending processes have been found to be biased against certain minority groups, leading to discrimination in the workplace and in access to credit. (<https://cmr.berkeley.edu/2020/11/algorithmic-bias/>)

1. The implications of AI failing in accordance with the GDPR can result in significant consequences for organizations, including fines and reputational damage. For example, if an AI system is found to have processed personal data in a manner that is not in accordance with the principles of accuracy, purpose limitation, and consent, this would be a violation of the GDPR. Additionally, if an AI system is found to have made automated decisions that have a significant impact on individuals and their rights, without giving them the option to opt-in or opt-out, this would also be a violation of the GDPR. In these cases, organizations may be required to pay fines or compensate individuals for any harm caused by the processing of their personal data. Ultimately, it is important for organizations to ensure that their AI systems are in compliance with the GDPR and to have robust governance and accountability frameworks in place to minimize the risk of violations and to ensure that AI is used responsibly and ethically. (<https://montrealethics.ai/the-impact-of-the-gdpr-on-artificial-intelligence/#:~:text=AI%20in%20the%20GDPR%3A%20Unlike,autonomous%20systems%2C%20intelligent%20systems%2C%20automated>)

Extension task:

Organizations should take the following steps to ensure that they are being responsible with AI and the wider use of data:

1. Ensure that individuals are provided with clear and concise information about the use of their personal data, including the purpose of processing, the data collected, and their rights under the GDPR.
2. Provide training and support to employees on data protection and privacy, and establish a culture of privacy and security within the organization.
3. Ensure that individuals have the right to opt-in or opt-out of automated decision-making processes that may have a significant impact on their rights and freedoms.
4. Implement robust privacy and data protection policies, which include data minimization, purpose limitation, accuracy, and security measures.
5. Collaborate with privacy and data protection experts, industry groups, and regulators to ensure that AI and data processing practices are aligned with the latest privacy and data protection standards and requirements.