Data Ethics Policy

1. BACKGROUND AND OBJECTIVE

Genmab is an international biotechnology company with a core purpose guiding its unstoppable team to improve the lives of patients through innovative and differentiated antibody therapeutics.

The use of Data, both personal and non-personal, is essential to fulfilling Genmab's core purpose; and Genmab is committed to handling Data with integrity and in an ethical and compliant manner considering the impact our actions may have on individuals and society.

Genmab is committed to following the IFPMA (International Federation of Pharmaceutical Manufacturers & Associations) Data Ethics principles when handling Data.

The IFPMA Data Ethics principles complement and strengthen already existing Genmab policies and procedures. These include the principles of Genmab's Code of Conduct, as well as the Genmab policies and processes governing areas of specific relevance for Data Ethics, such as Data Privacy, DE&I (Diversity, Equity & Inclusion), clinical trials and the review and approval by national ethics committees and particularly the process for review, design and application of new digital technologies (e.g., Artificial Intelligence, Machine Learning).

2. SCOPE

This Policy applies to all Genmab employees, consultants, contingent workers, and contractors when accessing and handling Data in connection with the provision of services to or on behalf of Genmab.

This Policy applies to all Data collected and used by or on behalf of Genmab. For the purpose of this Policy, "Data" is understood in its broadest sense and covers any information in any format, including numbers, quantities, characters, symbols, descriptions, facts, both personal and non-personal.

3. DATA ETHICS PRINCIPLES

To create a common framework and set the ethical standard for use of Data at Genmab we are committed to following the Data ethics principles established by IFPMA (International Federation of Pharmaceutical Manufacturers and Associations).

1. Autonomy: Respect individuals' privacy, protect their rights, and honor confidentiality. Data should be collected and used in ways that are consistent with the business intentions and with due understanding and respect of individual rights. Best efforts should be made to make individuals aware of how their Data will be used and, where appropriate and possible, offer them choices about who has access to their Data and how it may be used.

2. Transparency: Individuals should be able to understand how their personal Data are used. Individuals should be informed, in a manner that is appropriate and understandable to the relevant audience, regarding the type and extent of Data collected about them, how it will be used (including, to the extent possible, secondary uses of Data), how technologies are used to aid Data-based decisions that impact them, how their rights (including the right to privacy) are protected, and what actions they may take to exercise their rights. Legally permissible limitations on such rights should be clearly explained. Data governance standards and practices should be made available for public review, when appropriate.

3. Data quality: The best quality Data available should be used to make decisions. Data use should include processes to identify, prevent, and off-set poor quality, incomplete, or inaccurate Data. When Data quality, completeness, or accuracy presents risks of bias or harm to the individual, processes for mitigating these risks should be pursued and documented.

4. Fairness and non-discrimination: Data acquisition should be inclusive, equitable, and seek to support the industry's mission of responding to the needs of all patients. Engaging a diverse set of stakeholders in decision-making around Data use and development of technologies to leverage Data can build trust and support efforts to eliminate harmful biases. Technologies leveraging Data should also include Data-driven processes for quantifying the potential for bias in the populations in which they are being deployed.

5. Ethics by design: Controls to prevent harm and risks to individuals should be built into the design of Data architecture and Data processing. This includes having processes in place to identify, assess, and mitigate risks of intentional and unintentional discrimination and bias, breaches in privacy and security, physical harm, and other adverse impacts on individuals. Protecting privacy also includes applying strong cybersecurity standards (as well as notifying individuals when their Data is breached, where the risk to the individual is deemed high) and appropriately preparing the Data for use (e.g., anonymization and pseudonymization techniques where relevant) and restricting re-identification of anonymized Data without permission.

6. Responsible Data sharing: Data sharing should be based on processes that actively and consistently consider, prioritize, and protect individual rights. Data should always be obtained by legitimate means, and there should be designated individuals accountable for protecting and securing confidentiality of Data. Third parties working with Genmab should be informed about and expected to adhere to these principles. In addition, Data interoperability initiatives should prioritize, include, and support ethical and responsible Data sharing practices.

7. Responsibility and Accountability: Data Ethics Principles should be operationalized through effective governance, clear standards, training, monitoring activities, and disciplinary sanctions. Heads of Department should be aware, and ensure the application, of ethics principles in decisions around the use of Data in strategic activities.

Last updated: December 2022