Please see our GDPR terms below;

1. Data subject: Refers to the individual whose personal data is being processed.
2. Personal data: Any information that can directly or indirectly identify a person, such as their name, address, email, or IP address.
3. Data controller: The organization or entity that determines the purposes and means of processing personal data.
4. Data processor: The organization or entity that processes personal data on behalf of the data controller.
5. Data protection officer (DPO): A person appointed by an organization to oversee GDPR compliance and ensure that personal data is processed lawfully and appropriately.
6. Processing: Any operation performed on personal data, including collecting, storing, using, and transmitting the data.
7. Consent: The lawful basis for processing personal data, obtained through a clear affirmative action by the data subject.
8. Data breach: Any unauthorized or accidental access, disclosure, or destruction of personal data.
9. Right to erasure (also known as the "right to be forgotten"): The right of a data subject to have their personal data deleted or removed from a company's systems.
10. GDPR fines: Monetary penalties that can be imposed on organizations for non-compliance with GDPR requirements, which can reach up to €20 million or 4% of a company's global annual revenue (whichever is greater).
11. Privacy policy: A document that explains how an organization collects, uses, stores, and protects personal data. It also outlines the rights of data subjects and how they can exercise those rights.
12. Data protection impact assessment (DPIA): An assessment conducted by organizations to identify and mitigate privacy risks associated with their processing activities.

13. Data portability: The right of a data subject to receive a copy of their personal data in a structured, commonly used, and machine-readable format, and to transmit that data to another controller.

14. Privacy by design: A concept that calls for privacy considerations to be integrated into the design and development of products and services, rather than added as an afterthought.

15. Data minimization: A principle that calls for organizations to limit the amount of personal data they collect and process to only what is necessary for their stated purposes.

16. Sensitive personal data: A category of personal data that is considered particularly sensitive, such as information about a person's health, race, religion, or sexual orientation.

17. Supervisory authority: A regulatory body responsible for enforcing data protection laws and regulations within a particular jurisdiction.

18. Data subject access request (DSAR): A request made by a data subject to access their personal data held by an organization, and to exercise their rights under GDPR.