onetrust
DataGuidance

The Ultimate Guide to the GDPR

E-BOOK | MARCH, 2023

Table of Contents

Introduction

The General Data Protection Regulation (GDPR) is an EU law that was adopted by the Council of the European Union and the European Parliament in April 2016 and entered into effect on May 25, 2018. The regulation outlines a set of aims, key definitions, fundamental principles, data subject rights, controller and processor obligations, and penalties, among other things, across 11 chapters and 99 articles.

The GDPR aims to protect the fundamental rights and freedoms of individuals with respect to the protection of personal data. The GDPR establishes rules for organizations to adhere to when processing personal data in the EU or the personal data of EU citizens and promotes the free movement of personal data within the EU.

Background to the GDPR

The roots of the GDPR can be traced back to the adoption of the Universal Declaration of Human Rights in 1948 which set standards for which all people should be treated, which included the right to a private life and the right to freedom of expression.

General principles for data protection were first outlined in 1980 by the Organization for Economic Co-operation and Development (OECD) within its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines). The basic principles of the OECD Guidelines include collection limitation, data quality, purpose specification, use limitation, and accountability and are mirrored in the processing principles found under the GDPR.

The Council of Europe introduced the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) in 1981 - the first international, legally binding instrument on data protection. Signatories of Convention 108 are required to protect personal data from the risks associated with its collection and processing. Many elements of Convention 108 are echoed in the GDPR such as the prohibition on processing sensitive personal data and data subject rights including the right to be informed. In 2018, Convention 108+ was adopted, overhauling the provisions of Convention 108 to align more closely with the GDPR.

Several principles found under Convention 108 were used as a benchmark for the EU Data Protection Directive 1995 (the Directive). The Directive acted as a framework for EU Member States to regulate the collection, use, storage, disclosure, and destruction of personal data. EU Member States were required to transpose and implement the Directive into national law. Member State implementation meant that the interpretation of data protection law across the EU differed from country to country.

In 2016, the GDPR was introduced replacing the Directive and harmonizing data protection law across the EU by applying one set of requirements that apply across the region. The GDPR became enforceable on May 25, 2018.

Key definitions under the GDPR

Personal data

Personal data is defined by the GDPR as any information relating to an identified or identifiable natural person.

The GDPR further defines an identifiable natural person as an individual that can be identified by reference to information such as name, personal identification numbers, and online identifiers, such as IP address), among other things.

Processing

Processing is defined as any operation or set of operations that are performed on personal data. This includes collecting, organizing, storing, and disseminating personal data, among other things.

Data controller

A data controller is an entity that determines the purposes and means of processing personal data. A data controller can make this determination alone or jointly with others.

Data processor

A data processor is an entity that processes personal data on behalf of a data controller.

Pseudonymization

The GDPR defines pseudonymization as processing personal data in a way that it can no longer be attached to a specific data subject without additional identifiers. Any additional identifiers must be kept separate with adequate technical and organizational measures to ensure their security.

Important concepts under the GDPR

Data Protection Impact Assessment

Data controllers are required to conduct risk assessments known as a Data Protection Impact Assessment (DPIA) before commencing processing activities that:

- Use new technologies
- Are likely to result in a high risk to the rights and freedoms of natural persons
- Make decisions based on automated processing, including profiling
- Process large quantities of special category data or data relating to criminal offences
- Systematically monitor publicly accessible areas on a large scale

Data controllers are also required to consult the data protection officer (DPO), where applicable, when carrying out the DPIA and must include specific information outlined in Article 35(7) in the assessment.

Data Protection by Design and Default

Article 25 of the GDPR outlines the concept of Data Protection by Design and by Default. Data controllers are required to implement appropriate technical and organizational measures at the outset of a project to ensure that data protection principles such as data minimization are embedded into the activity by design.

Data Protection by Default requires data controllers to ensure that measures to facilitate a high level of data protection, such as retention policies, are set by default.

Data Protection Officer (DPO)

Data controllers and data processors that fall under the scope of the GDPR must designate a Data Protection Officer (DPO) if their activities meet any of the conditions outlined in Article 37(1).

The responsibilities of the DPO include:

- Informing and advising the data controller or data processor of their obligations in relation to the GDPR,
- Monitoring compliance with the GDPR
- Assigning responsibilities
- Training of staff involved in processing operations
- Providing advice with DPIAs
- Cooperation with the supervisory authority

Data controllers and data processors must ensure that the DPO does not receive any instructions regarding their tasks.

Furthermore, the DPO cannot be dismissed or penalized for performing his task and should report to the highest level of management.

Records of processing activities

Under Article 30 of the GDPR, data controllers are required to keep records of their processing activities. The records must be kept in an electronic format and should include the information outlined in Article 30(1). Data controllers must make the records of processing activities available to the relevant supervisory authority upon request.

Who does the GDPR apply to?

Who does the GDPR apply to?

The GDPR has a broad scope of application for the protection of personal data. The GDPR's scope of application defines whose personal data is covered, what personal data is protected, and considers the location of the data subject and data controller during processing activities. This is known as the personal, material, and territorial scope of the GDPR.

Personal scope

The personal scope of the GDPR applies to natural persons in relation to the processing of their personal data. The personal scope of the GDPR does not cover the personal data of legal persons or undertakings established as legal persons.

Material scope

The GDPR applies to personal data that is wholly or partly processed by automated means. It also applies to the personal data by non-automated means which forms part of a filing system or is intended to form part of a filing system.

The material scope of the GDPR explicitly highlights certain activities that do not fall under its scope. These include processing that takes place for purely personal or household purposes and the prevention, investigation, detection, or prosecution of criminal offenses, among other things.

Territorial scope

The GDPR applies to the processing of personal data by a data controller or data processor that is established in the EU. The GDPR applies regardless of whether the processing takes place in the EU.

The territorial scope of the GDPR also covers the processing of personal data of data subjects who are in the EU by a controller or processor established elsewhere. This includes offering goods or services to data subjects in the EU and monitoring the behavior of data subjects where that behavior takes place within the EU.

Additionally, the territorial scope of the GDPR applies to processing activities that are carried out by a data controller that is not established in the EU but is established in a jurisdiction where member state law applies by virtue of public international law.

Who does the GDPR apply to?

What is special category personal data?

Article 9(1) of the GDPR prohibits the processing of certain types of sensitive data. This is known as special category personal data. Examples of special category personal data include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data to uniquely identify a natural person
- Health data
- Sex life or sexual orientation

Data controllers are strictly prohibited from the processing of special categories of personal data unless an exception listed in Article 9(2) applies. These include:

- Where the data subject has explicitly given consent
- When processing is necessary to protect the vital interests of the data subject
- In cases where the personal data has been made public by the data subject
- When processing is necessary for the establishment, exercise, or defence of legal claims
- When processing is necessary for reasons of public interest in the area of public health

What are the 7 principles of the GDPR?

The GDPR sets out seven fundamental principles relating to the processing of personal data that data controllers should follow.

1. Lawfulness, fairness, and transparency

The lawfulness, fairness, and transparency principle is fairly clear-cut. Data controllers must process the personal data of the data subject is lawful, fair, and transparent manner.

2. Purpose limitation

Purpose limitation means that personal data should be collected for a specific and legitimate purpose. It also means that personal data should not be processed for any other purposes than those explicitly outlined at the time of collection.

3. Data minimization

Data controllers should ensure that the personal data they collect is adequate, relevant, and limited to what is necessary for the purposes of the processing activity.

4. Accuracy

Data controllers must take reasonable steps to ensure that the personal data they store is accurate and where possible kept up to date. Inaccurate data must be rectified or destroyed without undue delay.

5. Storage limitation

The storage limitation principle requires data controllers to store personal data for no longer than is necessary for the initial purposes for processing. Personal data can be stored beyond these purposes in limited circumstances including in the public interest, scientific or historical research purposes, or statistical purposes insofar as the appropriate organizational and technical measures have been implemented to protect the personal data.

6. Integrity and confidentiality

Data controllers should use appropriate technical and organizational measures to ensure adequate security is given to personal data in the course of processing. This includes protecting personal data against unauthorized or unlawful processing and accidental loss, destruction, or damage.

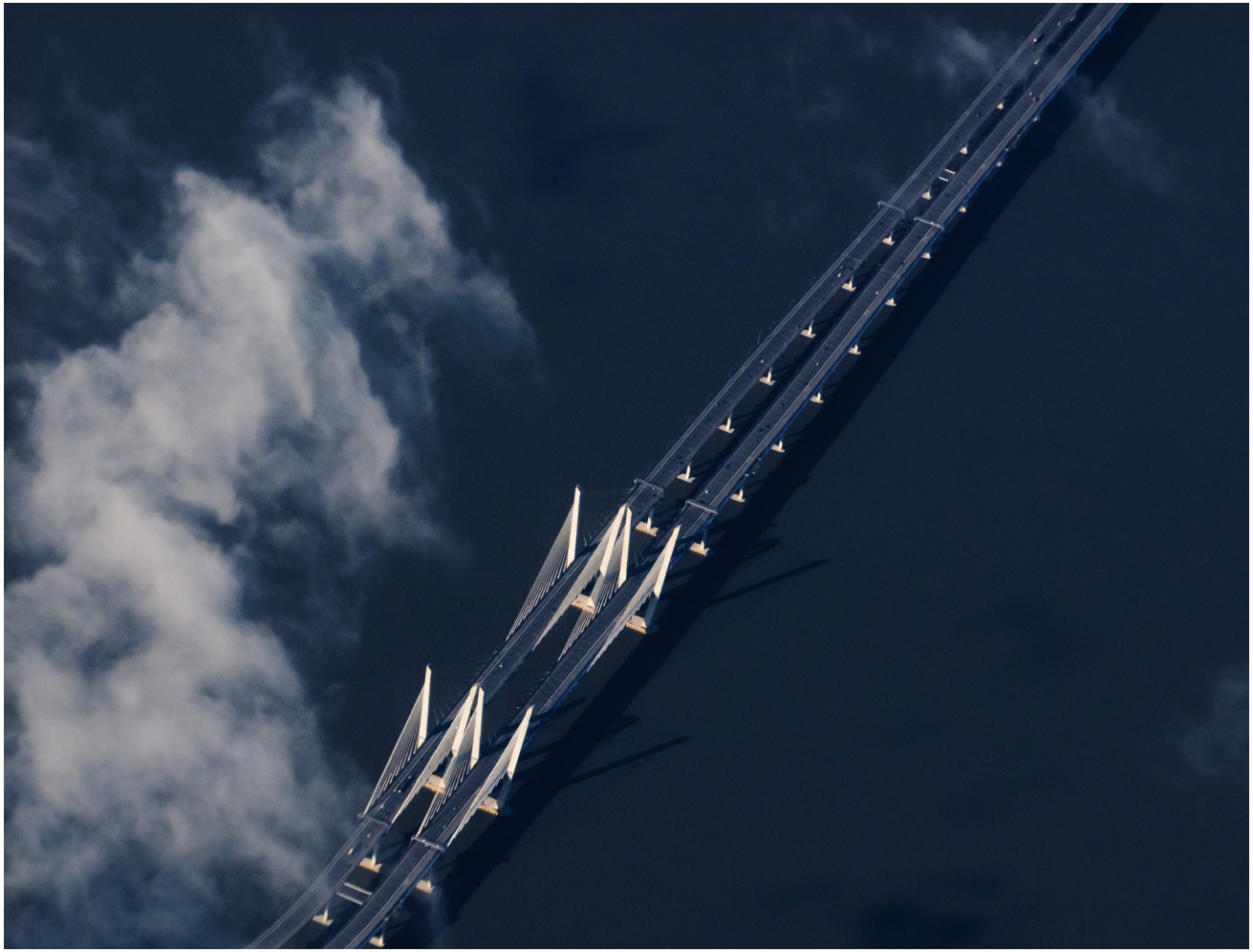
7. Accountability

The accountability principle holds the data controller responsible for being able to demonstrate compliance with the above principles.

What are the Legal Bases for Processing Personal Data under the GDPR?

Article 6 of the GDPR outlines the conditions for the lawful processing of personal data. Article 6 states that for the processing of personal data to be lawful, at least one of the following legal bases must apply:

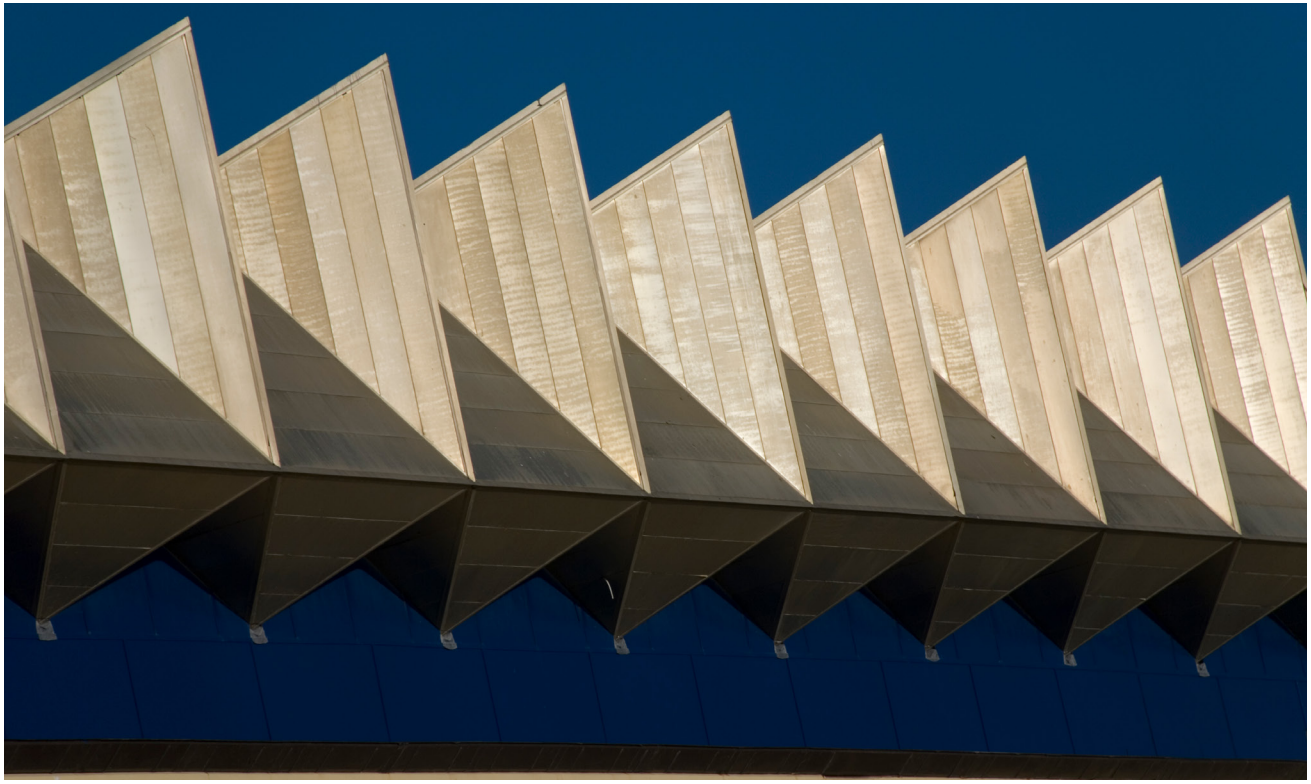
- The data subject has given consent for the processing to take place
- Processing is necessary for the performance of a contract
- Compliance with a legal obligation
- To protect the vital interests of the data subject
- Performance of a task carried out in the public interest
- There is a legitimate interest
- Public authorities are unable to rely on legitimate interest as a legal basis for processing personal information.



What is consent under the GDPR?

Consent under the GDPR is one of the most common legal bases that data controllers rely upon. However, the GDPR outlines specific conditions that need to be met for consent to be deemed valid. Firstly, it is important to look at how the GDPR defines consent: 'consent' of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Article 7 of the GDPR also outlines the conditions that need to be met for consent to be valid. Under Article 7's conditions for consent, the data controller must be able to show that the data subject has given their consent for the processing activity. Furthermore, the data subject must be able to withdraw consent as easily as it is given at any time and must be informed of this right before consent is collected.



Further conditions for consent under the GDPR include presenting the request for consent in a clearly distinguishable manner in an intelligible and easily accessible form that uses clear and plain language. Data controllers must also consider whether the consent is freely given or whether the performance of a contract is conditional on the data subject giving consent.

What are GDPR Data Subject Rights?

The GDPR offers data subjects several rights in relation to their personal data as outlined in Chapter 3. There are also several requirements that data controllers need to meet under Chapter 3 including the transparent communication of a data subject's rights and the methods for submitting requests.

Chapter 3 outlines that data controllers must respond to data subject rights request without undue delay and within one month from receipt of the request. Reponses to data subject rights request must be provided free of charge except where the request is found to be unfounded, excessive, or repetitive in nature.

Right to be informed

Data subjects have the right to be informed of the details of the data controller and data processor, the purposes for the processing of personal data, data subject rights under Articles 15 to 22 of the GDPR, and the legal basis the processing is relying on, among other things. The data controller must ensure this information is present on or before the time of collection and must be communicated in a concise, transparent, intelligible, and easily accessible form.

Right to access

Data subjects have the right to access information relating to the processing of their personal data from the data controller. This includes confirmation of whether or not the data subject personal data has been processed as well as the purposes of the processing, the categories of personal data concerned, and the recipients of the personal, among other things.

Right to rectification

Data subjects have the right to instruct data controllers to rectify inaccurate or incomplete data. The data controller must correct the information without undue delay.

Right to erasure

Also known as the right to be forgotten, data subjects have the right to instruct data controllers to erase personal data relating to them without undue delay.

What are GDPR Data Subject Rights?

Right to restriction of processing

Data subjects have the right to restrict the processing of their personal data if one of the following conditions are met:

- The accuracy of the personal data is contested by the data subject
- The processing is unlawful and the data subject opposes the erasure of the personal data
- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims
- The data subject has objected to processing on the grounds of a legitimate interest of the data controller pending the verification of whether the legitimate grounds of the controller override those of the data subject

Right to data portability

Data subjects have the right to request the personal data that they have provided a data controller in a structured, commonly used, and machine-readable format. Data subjects also have the right to transmit that data to another data controller without interference.

Right to object

Data subjects have the right to object to the processing of their personal data where the data controller is relying on legitimate interest, or the processing is necessary for the performance of a task in the public interest. The data controller must stop the processing unless it can demonstrate compelling legitimate ground which overrides the interests, rights, and freedoms of the data subject.

Right to not be subject to a decision based solely on automated processing

Data subjects have the right to not be subject to decisions based solely on automated processing, including profiling, which produces legal effects concerning the data subject.

GDPR enforcement and penalties

The GDPR outlines the conditions for transferring personal data outside of the EU in Chapter 5. General principles for the international transfer of personal data are outlined in Article 44 which states that such data transfers can only take place if the conditions of Chapter 5 are met.

Under the GDPR, data controllers and data processors can transfer personal data outside of the EU if:

- The transfer is made on the basis of a European Commission adequacy decision
- The transfer is subject to appropriate safeguards under Article 46, including:
- Standard Contractual Clauses (SCCs)
- Codes of conduct
- Approved certification mechanisms
- The transfer is subject to Binding Corporate Rules (BCRs)
- The transfer relies on a derogation

On July 16, 2020, the Court of Justice of the European Union (CJEU) published its judgment in the Schrems II case, which declared the EU-US Privacy Shield invalid. The judgment also cast doubt over the effectiveness of SCCs which led to the European Commission issuing a revised set of SCCs and the European Data Protection Board (EDPB) issuing guidance on the supplementary measures to ensure an EU level of data protection when transferring personal data to a third country.

Supervisory authority powers

The GDPR provides for the establishment of an independent and competent supervisory authority in each EU Member State to ensure the consistent application of the GDPR and to facilitate the free flow of data within the EU.

The GDPR also establishes a set of responsibilities that must be carried out by supervisory authorities. Article 57 outlines that supervisory authorities must monitor and enforce the application of the GDPR, promote public awareness of the GDPR, and handle complaints lodged by data subjects, among other things.

Article 58 of the GDPR establishes the powers granted to supervisory authorities which are presented in three categories: investigative powers; corrective powers; and authorization and advisory powers.

Investigative powers

Article 58(1) outlines the investigative powers granted to supervisory authorities, which include:

The power to carry out investigations in the form of data protection audits

The power to notify the controller or the processor of an alleged infringement of the GDPR

The power to obtain access to all personal data and to all information necessary for the performance of its tasks from a data controller or data processor

The power to access to any premises of data controllers and data processors

GDPR enforcement and penalties

Corrective powers
Article 58(2) outlines the corrective powers granted to supervisory authorities, which include:

The power to issue warnings that processing operations are likely to infringe provisions of the GDPR

The power to issue reprimands to data controllers or data processors where processing operations have infringed provisions of the GDPR

The power to order data controllers or data processors to bring their processing operations into compliance with the GDPR in a specified manner and within a specified period, where applicable

The power to order data controllers to communicate data breaches to the data subject

The power to impose a temporary or definitive limitation including a ban on processing

The power to impose an administrative fine

The power to order the suspension of data transfer to a recipient in a third country or to an international organization

Authorization and advisory powers
Article 58(3) outlines the authorization and advisory powers granted to supervisory authorities, which include:

The power to advise the controller in accordance with the prior consultation procedure (Article 36)

The power to authorize processing where a data controller is acting in the public interest

The power to issue an opinion and approve draft codes of conduct

The power to authorize contractual clauses referred to in Article 46

The power to approve binding corporate rules pursuant to Article 47

GDPR penalties
Article 83 of the GDPR sets out general conditions for supervisory authorities to issue administrative fines. The GDPR states the administrative fines handed down by the supervisory authority must be 'effective, proportionate, and dissuasive.'

When issuing administrative fines, supervisory authorities must consider a number of factors outlined by Article 83(2). These include: the nature, gravity and duration of the infringement; whether the infringement was intentional or negligent in nature; the actions taken by the data controller or data processor to mitigate the damage; and the categories of personal data affected.

Depending on the nature of the violation, supervisory authorities can issue administrative fines for infringements of the GDPR ranging up to €10 million or 2% of global turnover of the preceding financial year, whichever is greater or €20 million or 4% of global turnover of the preceding financial year, whichever is greater.

11 Steps to GDPR compliance

GDPR compliance can look different depending on the type and size of the business you operate. However, there are several steps any business can take to build the foundations of a GDPR compliant privacy program.

1. Develop a plan of action using the seven principles of the GDPR
2. Create a record of processing activities per Article 30
3. Implement Privacy by Design and processes for conducting DPIAs
4. Develop a framework for consent management
5. Understand requirements for cookie consent in the countries that you operate
6. Create a portal for data subject rights requests intake
7. Review risks from data processors
8. Prepare an incident management plan
9. Review mechanisms for international data transfers
10. Roll out GDPR training programs
11. Appoint a DPO, where applicable

onetrust
DataGuidance

About OneTrust DataGuidance™

OneTrust DataGuidance™ is an in-depth and up-to-date privacy and security regulatory research platform powered by more than two decades of global privacy law research. Hundreds of global privacy laws and over ten thousand additional resources are mapped into DataGuidance to give customers in-depth research, information, insight and perspectives on the world's evolving list of global privacy regulations. The database is updated daily by over 40 in-house privacy researchers, along with a network of 800 lawyers across over 300 jurisdictions, and by active input as part of OneTrust's regulatory engagement program.

OneTrust DataGuidance is a part of OneTrust, the #1 most widely used privacy, security, and governance platform used by more than 8,000 customers and powered by 150 awarded patents. OneTrust DataGuidance fuels the intelligence for the OneTrust Athena™ AI and robotic automation engine, and integrates seamlessly with the full OneTrust platform, including OneTrust Privacy Management Software, OneTrust DataDiscovery™, OneTrust DataGovernance™, OneTrust Vendorpedia™, OneTrust GRC, OneTrust Ethics, OneTrust PreferenceChoice™, and OneTrust ESG.

In 2020, OneTrust was named the #1 fastest growing company on the Inc. 500. According to the IDC Worldwide Data Privacy Management Software Market Shares Report, 2020, "OneTrust is leading the market outright and showing no signs of slowing down or stopping." OneTrust has raised a total of $920 million in funding at a $5.3 billion valuation from Insight Partners, Coatue, TCV, SoftBank Vision Fund 2, and Franklin Templeton.

OneTrust's fast-growing team of 2,000 employees is co-headquartered in Atlanta and London with additional offices in Bangalore, Melbourne, Denver, Seattle, San Francisco, New York, São Paulo, Munich, Paris, Hong Kong, and Bangkok.

To learn more, visit DataGuidance.com or connect on LinkedIn.