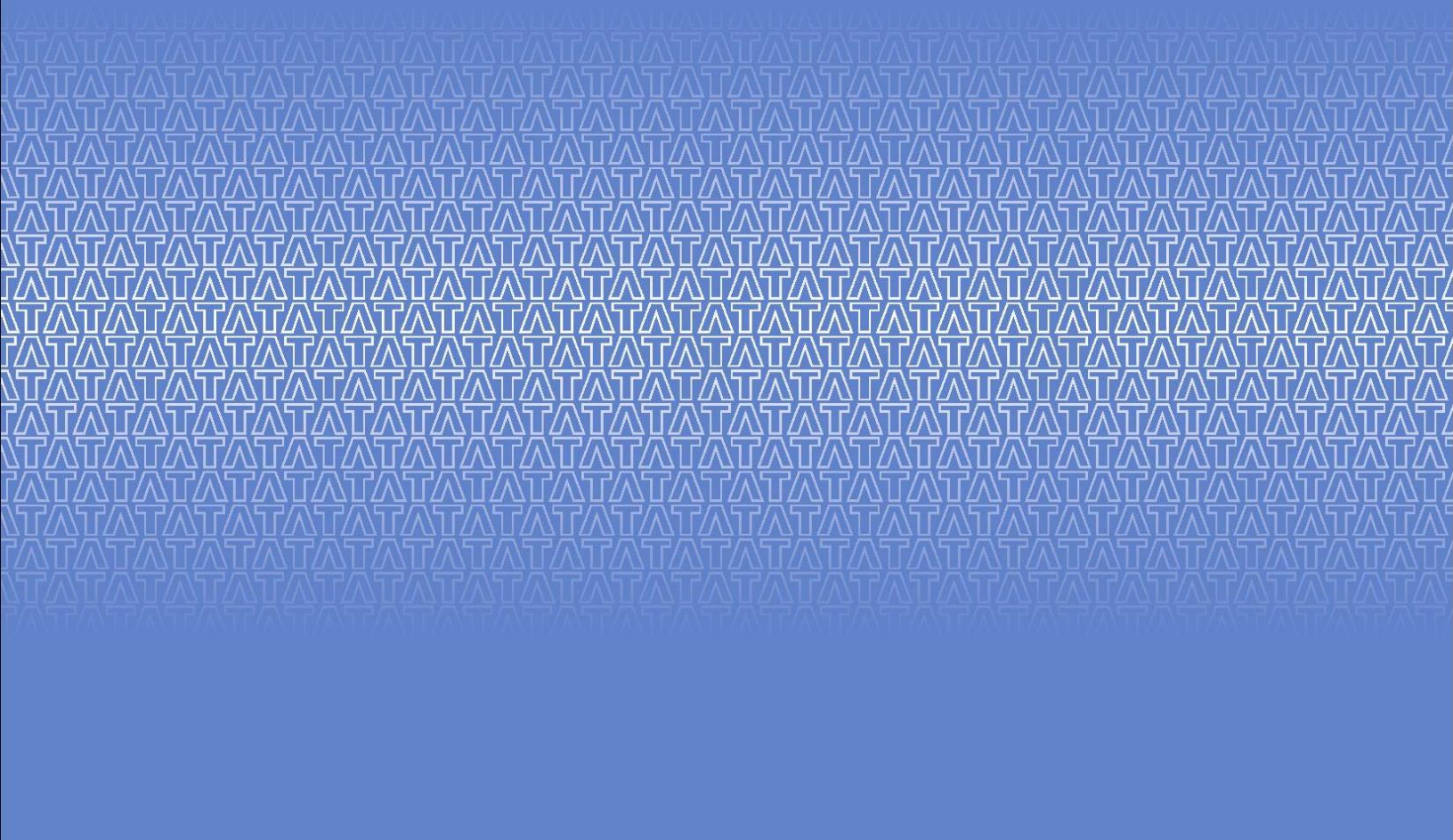
TATA CONSULTANCY SERVICES

Experience certainty.

IT Services
Business Solutions
Outsourcing



Notice
This is a controlled document. Unauthorized access, copying, replication or usage for a purpose other than for which it is intended, are prohibited.

Here are some key terms that you will keep coming across in GDPR.

GDPR: People

- Data Subject: is a living person who can be directly or indirectly identified by the Controller or a third party by his or her data. In the above example, the personal data of a TCS associate is being collected for organization needs, and the associate is the Data Subject.
- Data Controller: a person or a group of people who determine the purpose and the manner in which any personal data is collected and processed. The data controller will then need the consent of the data subject to use the data for the specified purpose. Here TCS is the Data Controller for its employee data.
- Data Processor: a person or a group of people who process the data on behalf of the Data Controller. Here, the processing means obtaining, recording or holding the data or carrying out any operation or set of operations on the data. So, in this scenario the travel agency is the Data Processor.

Supervisory Authority: Data protection regulators are referred to as supervisory authorities. A single lead supervisory authority located in the Member State in which an organization has its "main" establishment will regulate that organization's compliance with the GDPR.

Data Protection Officer (DPO): Controllers and Processors are free to appoint a DPO for monitoring and controlling their organization's GDPR compliance, including training and awareness raising, running audits, advising regarding PIAs and liaising with supervisory authorities. The DPO's contact details must be published and also notified to an organization's supervisory authority as the DPO is to be a point of contact for questions about data protection compliance matters. With GDPR coming into force, DPO not only needs to 'advice' but is obliged to 'control' as well.

GDPR: Data

Personal Data: Any data by which a living person (Data Subject) can be identified, directly or indirectly.

Sensitive Personal Data: Special categories of Personal Data (called sensitive data) which are processed "to uniquely identify a person" are considered Sensitive. These include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Data concerning health or sex life and sexual orientation

GDPR: Process

- Transfer of Personal Data: This is with respect to the transfer of personal data to countries outside the EU or to international organizations, which are not part of the whitelist of countries considered to be reasonably secure. The data does not need to be physically transported to be considered as transferred. Viewing the data hosted in another location would amount to a transfer for GDPR purposes.

- Consent of the Data Subject is freely given, specific, informed and unambiguous indication of his/her wishes by which he/she signifies agreement to the processing of personal data relating to him/her. The consent will be informed only where the Data Subject is aware of the identity of the Controller and the intended purpose of processing. The Data Subject must have the right to withdraw consent at any time. It is important that the consent is clear and explicit.

Data Breach: In case of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data a Data Breach will be triggered.

- Genetic and biometric data that is processed to uniquely identify a person is also considered to be Sensitive Personal Data.

Finally, let's understand what PIA is. Privacy Impact Assessment (PIA): is an assessment to identify and minimize non-compliance risks. Controllers must ensure that a PIA is run on any "high risk" processing activity before it is commenced. Here is a spider web example of the same.

Editable image:

Scope

EU "established" Data Controllers or Processors.

GDPR will apply to organizations (Data Controller and Processors) which have EU "establishments", where personal data is processed "in the context of the activities" of such an establishment. If this is met, GDPR applies irrespective of whether the actual data processing takes place in the EU or not.

Non-EU "established" organizations who target or monitor EU Data Subjects

Where no EU presence exists, GDPR will still apply whenever: (1) an EU resident's personal data is processed in connection with goods/services offered to him/her (2) the behavior of individuals within the EU is "monitored". Monitoring specifically includes the tracking of individuals to create profiles, including where this is used to take decisions to analyze/predict personal preferences, behaviors, attitudes etc.

Exclusion

GDPR does not apply to certain activities – including processing covered by the Law Enforcement Agencies ("LEA") Directive, for national security purposes and processing carried out by individuals purely for personal/household activities.

Also, any data that is not personal data is outside the scope of the proposed regulation.