virtusa
Accelerating Business Outcomes

General Data Protection Regulation (GDPR) for European Union Guidelines

JUNE 2018

Version:

Approved by:

Release Date:

Agenda

- Overview of Data Privacy
- Introduction to General Data Protection Regulation (GDPR)
- Key GDPR requirements
- Implications of Non-compliance
- Expectations from you
- Privacy Notice to Employees & Sub-Contractors

Overview of Data Privacy

Privacy For Virtusa

Why Data Privacy for Virtusa?

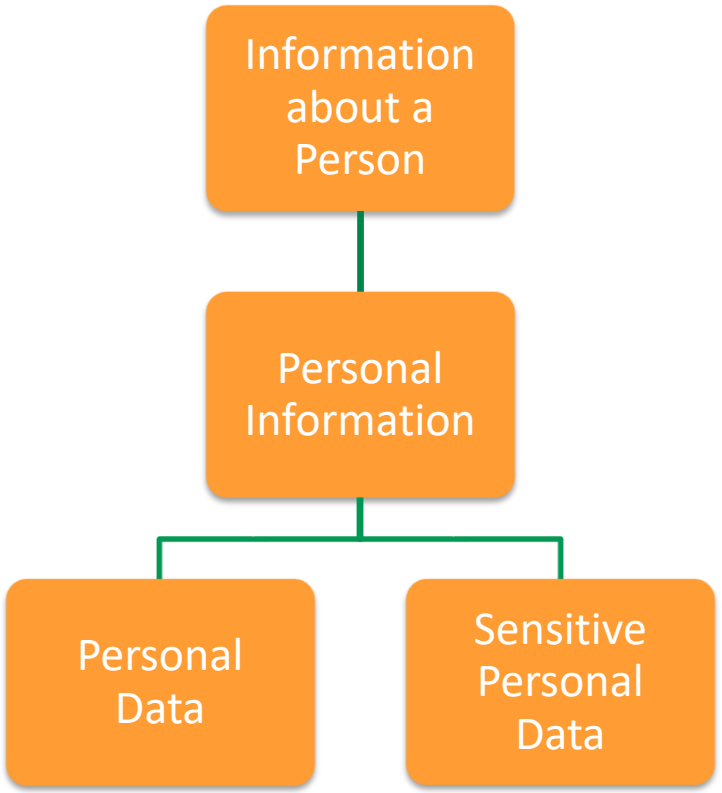
- Virtusa collects/ uses/ stores/ handles personal information of individuals (such as employees, customers, visitors, employment candidates, contractors etc.) as part of its operations.
- The organization operates in multiple geographies.
- Every geography has specific data privacy laws and regulatory requirements which need to be complied with.

What we aim to achieve?

- A robust privacy program to ensure that:
  - Virtusa's reputation is protected
  - We comply with privacy requirements
  - We comply with contractual requirements
  - Privacy compliance becomes a part of everyday behavior
- Employee compliance with privacy standards such that:
  - They understand the potential impact for the organization
  - Understand their role and responsibilities for compliance to privacy
- Assurance to stakeholders and regulators
- Decreased cost of non-compliance

Overview

In the most general terms, privacy is the 'ability to control how you are identified, contacted, and located'. It also gives you control over how your information may be collected, used, processed and stored by organizations.



Personal Data

- 'Personal data' refers to any information relating to an identified or identifiable natural person ('data subject'). An 'identifiable' person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier; or, to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Sensitive Personal Data (known as special categories of personal data under GDPR)

- 'Sensitive Personal Data' refers to personal data about the: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; and genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately.

Note: As defined within GDPR

Examples of Personal Data Elements

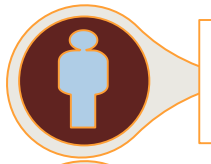
Personal Data or PII

- Name
- Gender
- Age and date of birth
- Marital status
- Citizenship
- Nationality
- Languages spoken
- Disabled status
- Business and personal address
- Business and personal phone number
- Business and personal email address
- Internal identification numbers
- Government-issued identification numbers
- Identity verification information

Special categories of personal data or SPII

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual life or sexual orientation
- Genetic data
- Biometric data
- Health data

Key Privacy Terms



Personal Data (PII): Any information relating to an identified or identifiable natural person ("data subject").

Special Categories of Personal Data (SPII): "Sensitive data" that can only be processed under strict limited exceptions, such as express consent or necessity for vital interests of a data subject.

Processing: Any operation that is performed on personal data, whether or not by automated means.

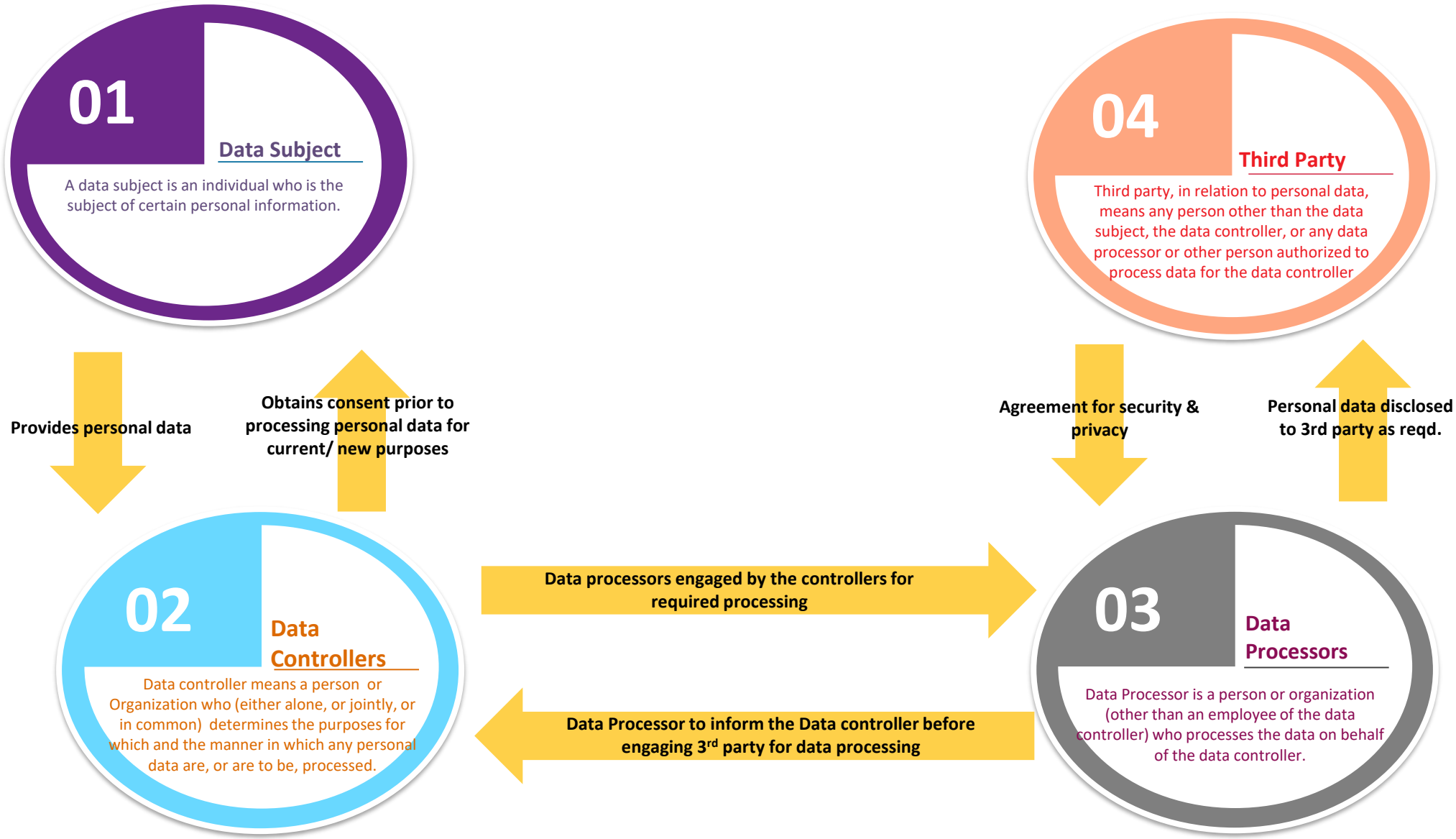
Data Controller: Entity that makes the decisions about how personal data is processed.

Data Processor: Entity that carries out the controller's decisions regarding processing of personal data.

Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Supervisory Authority: An enforcement body in each Member-State that monitors compliance with EU data protection laws on a national level.

Privacy Ecosystem

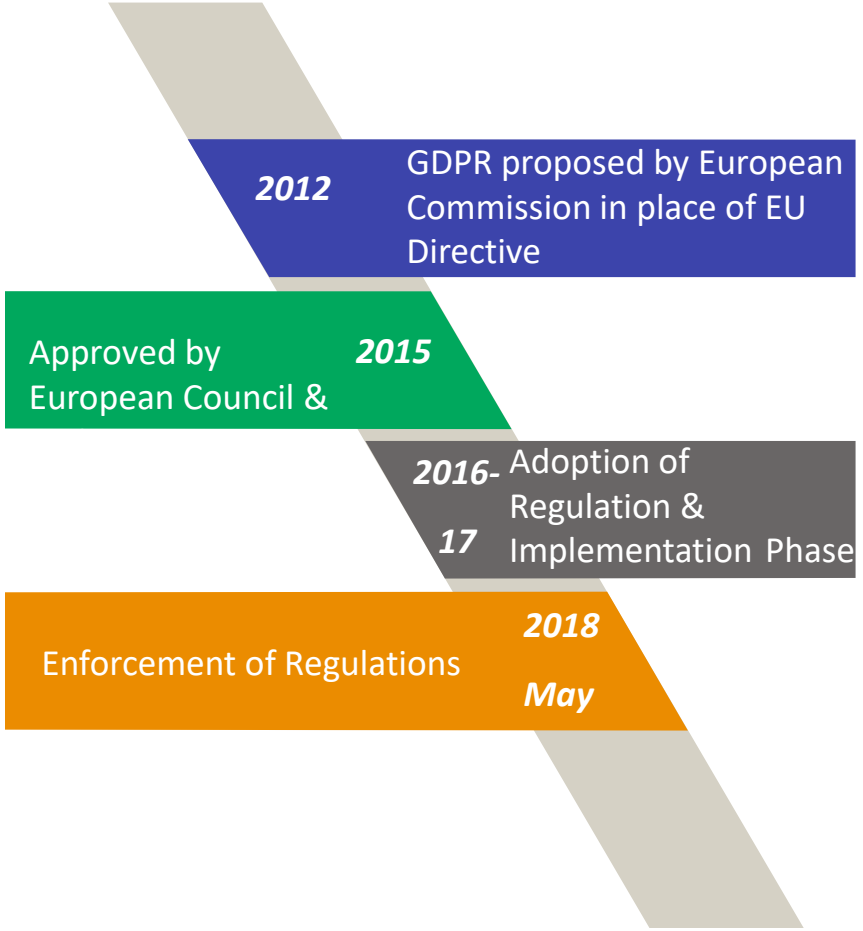


Introduction to GDPR

What is GDPR?

The General Data Protection Regulation, which was finally adopted in April 2016 in the European Parliament, represents a Big Bang in terms of the regulation of personal data protection in Europe.

- **Aim:** To harmonize Data Protection directive & strengthen citizens' fundamental rights to personal data protection.
- **Enforcement date**: 25th May, 2018
- **Applicability:** Every entity that holds or uses European personal data both inside and outside Europe.



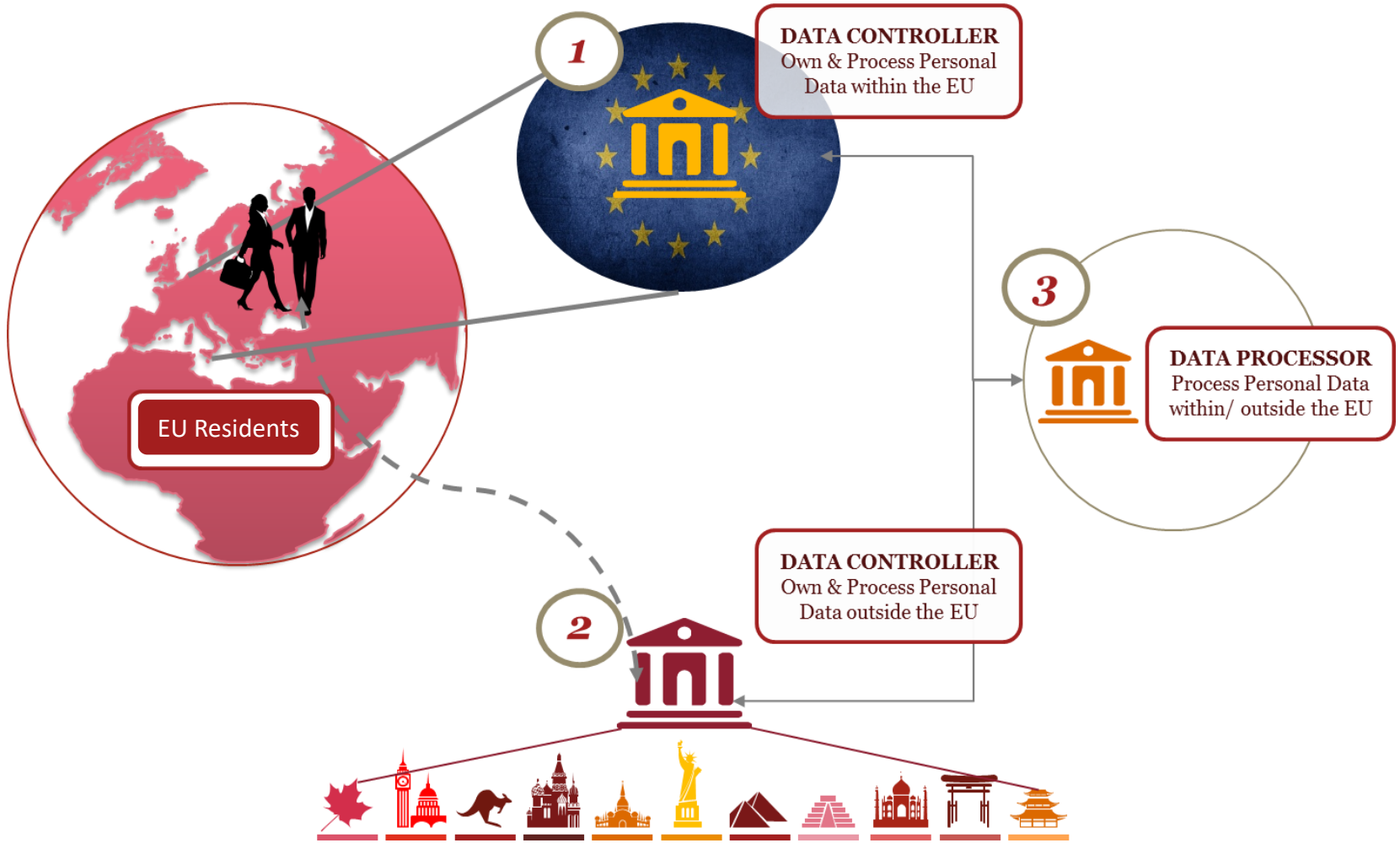
Enforcement and Liabilities

Major infringements: higher of EUR 20 Million or 4% of the worldwide annual turnover

Other infringements: higher of EUR 10 Million or up to 2% of the worldwide annual turnover

Is GDPR applicable to you?

In cases where EU residents data is accessed/processed by your firm as a data controller/processor within or outside EU, then GDPR is applicable.



Key GDPR requirements

Key Highlights

Enforcement and Liabilities	Major infringements : higher of EUR 20 Million or 4% of the worldwide annual turnover Other infringements : higher EUR 10 Million or up to 2% of the worldwide annual turnover
Data Subject Rights	New rights to be forgotten, erasure and data portability. Right to object to processing is broader, allowing to object to processing at any time, unless the controller has compelling legitimate grounds. Special provisions for children
Data Protection by Design	Applies to controllers but not to processors. Embed data privacy into practices and systems and consider data protection requirements & risks at all stages of the data life-cycle.
Accountability	Controllers to implement measures to ensure and demonstrate that data processing is compliant with GDPR Measures in each case to depend on the nature, scope, context and purposes of the relevant processing as well as the risks for rights and freedoms of individuals.
Data Processor Obligations	GDPR imposes compliance obligations directly on data processors and holds them directly liable for non-compliance of those obligations such as record processing activities, perform DPIAs for high risk processing, inform data breach to controller etc. The new processor obligations will equally apply to processors not established in the EU
Data Protection Impact Assessment	Controllers shall carry out a DPIA for data processing likely to result in a high risk for the rights and freedoms of individuals Processors should assist controllers, where necessary and upon request, in complying with these obligations
Explicit Consent	Clear affirmative action is needed. Silence, pre-ticked boxes and inactivity will no longer suffice. Pre-GDPR consents will continue to be valid provided they conform to the GDPR requirements.
Profiling	Profiling is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person. Data Subjects have a right not to be subject to a decision based solely on profiling (or other automated processing activities) which produces legal effects concerning them or similarly significantly affects them.

Key Highlights

Data Mapping	It is mandatory for Data Controllers to have accurate data maps addressing details such as 'Who/ Where/ What/ When/ Why' of Personal Data under their control.
Data Protection Officer	All public sector bodies to designate a DPO. Private sector controllers and processors must appoint a DPO if their core activities include: processing operations requiring regular and systematic monitoring of data subjects on a large scale; or processing on a large scale of special categories of data such as criminal convictions and offences.
Cross-Border Data Transfer Rules	Rules from the EU Directive are retained. As per the GDPR, Binding Corporate Rules (BCRs) allow groups of companies to make intra-organizational transfers of personal data across borders given that requirements of GDPR are met. BCRs will be formally recognized as measures citing appropriate safeguards and will be subject to uniform rules when it comes to their adoption.
Data Breach Notification Obligations	Notify a personal data breach to competent SA without undue delay not later than 72 hours Communicate a personal data breach to data subjects without undue delay

Implications of Non-compliance

Key Challenges

Personal Information of employees, vendors, customers, customers' customer etc.

Complex requirements such as Right to be Forgotten, Right to Data Portability, DPIA etc.

Increased obligations on Data Processors

Outsourcing, off-shoring, and extended global enterprises

Profiling

Corporate reputation

Implication of Non-Compliance

- Regulatory action
- Litigation
- Increased cost of compliance

- Loss of Customer and business partner confidence
- Brand and reputation damage
- Loss of market value
- Direct financial loss

Penalties for Non-compliance

Tier 1: Higher of **EUR 10,000,000** or up to **2% of the worldwide annual turnover of the preceding financial year**

Infringement
Failure to obtain parental consent where information society services are offered to children below the age of consent
Failure to adhere to data protection by design/data protection by default principles
Failure to designate a representative in the EU in case not established in the EU
Failure to maintain adequate processing records
Failure to implement appropriate security measures
Failure to notify data breaches as required
Failure to carry out DPIAs as required or consult with SA on high-risk processing
Failure to appoint a DPO (if mandated)
Failure to comply with certification requirements

Tier 2: Higher of **EUR 20,000,000** or up to **4% of the worldwide annual turnover of the preceding financial year**

Infringement
Failure to comply with the basic processing principles, including conditions for consent
Failure to comply with data subjects' rights
Failure to comply with cross-border transfer principles
Failure to comply with any obligations adopted pursuant to Member State law
Failure to allow SA access to personal data and/ or premises in order to exercise its investigative powers
Failure to comply with an order issued by a SA in exercising its corrective powers

Expectations from you

General expectations from employees

1

Be aware of the sensitivity of the personal data in your custody.

2

Be sensitive to who has access to the personal information and data.

3

Protect the confidentiality of personal information handled by you (such as personal data of employees, employment candidates, clients, end customers etc).

4

Notify the data privacy officer dpooffice@virtusa.com in your firm about any data privacy breach.

Personal Data Breach Notification

Overview: A personal data breach is ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.’

It applies to all personal data, meaning ‘any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier etc.’

The breach could happen in the context of our client services (such as business processing operations, applications support etc.) and internal operations (such as HR operations). When, how and to whom we provide notice depends on whether we are a controller or processor, and on the risk of harm arising from the breach.

Consequences of Non-Compliance

COMPANY

Virtusa's reputation, goodwill, and brand image may be damaged.

Virtusa may be held responsible for the breach of obligations to clients.

Virtusa could lose one or more clients.

Virtusa could be subject to civil and criminal penalties.

EMPLOYEE

You may face disciplinary action, which can even lead to termination of employment.

You may be subject to civil and criminal penalties.

Privacy Notice to Employees and Sub-Contractors

*Note: Benefits are applicable only for employees

Privacy Notice to Employees and Sub-Contractors

Personal data collection

We collect and maintain the below categories of personal data and sensitive personal data of our employees & sub-contractors. The personal data collected may include but is not limited to:

- **Identification Information** including name, age, date of birth, email address, home address, contact details, government-issued identification numbers, photographs, demographic information, citizenship, nationality, marital status, etc.
- **Educational and Professional Details** including higher education, certifications, previous employment history, etc.,
- **Background check reports** including educational and employment checks, etc. in accordance with applicable law(s)
- **Compensation and Benefits Information** including details of salary and benefits, name & contact details of family member's or dependents, bank account details, salary reviews, records relating to holiday and other leave(s), working time records etc.
- **Child Care Vouchers** - We provide certain benefits such as payment of childcare center fees to working parents. In order to provide these benefits, we require information related to your child/children such as name, date of birth, educational institution, fee and bills.
- **Information about your performance at work**, including references obtained from your previous place of work, performance evaluations, as well as opinions expressed by your colleagues, individuals whom you manage, supervisors, and clients of Virtusa;
- **Travel and Expenses Information** including passport, visa details, corporate card transactions, expense details, supporting bills, etc.
- **Learning and Development Information** including training, certifications, attendance and assessment records, etc.
- **Information collected as part of Surveillance and Monitoring** such as video surveillance data, physical access logs, activity logs from systems, communication channels, etc.

*Note: Benefits are applicable only for employees

Privacy Notice to Employees and Sub-Contractors

The sensitive personal data collected may include:

- **Information relating to your Health:** such as disability status, Biometric data, etc.
- **Information related to racial, ethnic origin or religious beliefs** to comply with local regulatory law(s).
- **Data relating to criminal convictions and offences** collected from background checks or CCTV monitoring.

Purposes of processing your personal data and the legal basis for processing

The personal information we hold and process about you, enables us to run the business and manage our relationship with you effectively. This information is collected and processed during the recruitment process, whilst you are working for us, at the time when your employment ends and after you have left. The purpose is to comply with your employment contract, any legal requirements, pursue our legitimate business interests and defend our position in legal proceedings. Some of the key processing activities shall include:

- **Pay your salary and register you for benefits** - The information requested is for the performance of our obligations under your employment contract.
- **Child Care Benefits** – We may process the personal data of your child/children only when you request for childcare services as a part of our benefits program.
- **Pay taxes** – We are legally obliged to pay certain taxes on your earnings and use your information for our legal obligations.
- **Background Verification** – We may engage third-party vendors to carry out background verification checks including identity, educational, employment and criminal verification to comply with applicable legal requirements and where permissible under local law.
- **Staff administration** – We may keep employment records relating to employment history, CV, references, absences, etc. We keep a copy of your employment contract and any correspondence with you in the event of termination of your employment, for our legitimate business interests and compliance with employment law.

*Note: Benefits are applicable only for employees

Privacy Notice to Employees and Sub-Contractors

- **Performance and compensation** – We may process personal data as part of performance review processes and in relation to compensation, rewards, and benefits. We also keep learning and development records for our legitimate business interests.
- **Travel and Expense** – We may process personal data and engage travel and immigration vendors in facilitating corporate travel, location transfers, validating expenses and relevant activities in line with our Travel, Mobility and Expense policies.
- **Discipline, grievance, and dismissal** – From time to time, we may process personal data in connection with disciplinary, grievance and dismissal processes, to satisfy our legitimate business interests.
- **Monitoring and Surveillance** - We monitor and record computer use and in certain cases, corporate telephone use and also carry out CCTV monitoring of key areas. We also keep records of your hours of work to satisfy our legitimate business interests, for the safety and security of the company and its staff.
- **Audit Compliance** – We may process the necessary personal data as part of our audit processes and engage third-party auditors to comply with applicable laws and to satisfy our legitimate business interests.
- **New employment opportunities** - We may retain your employment records and related documents containing your personal data for future employment-related opportunities.
- **Disclosure of business contacts, CV, and background screening information to clients** – where required by clients as data controllers.
- **Prevention of fraud** – We may process your personal data for the purpose of fraud prevention and the legitimate business interests.
- **Verifying compliance with Virtusa policies** – We may process your personal data for the purpose of assessing and ensuring your compliance with the various internal Virtusa policies in pursuit of the legitimate business interests of the company.
- **Reporting potential crimes** – We may process your personal data for detection and reporting potential crimes where required under national law(s).
- **Documents produced by employees & sub-contractors** – We may store documents and records that are produced by you and your colleagues which contain your personal data, may be shared with clients to carry out your duties and in pursuit of our legitimate business interests.

*Note: Benefits are applicable only for employees

Privacy Notice to Employees and Sub-Contractors

Sensitive personal data - We may process sensitive personal data relating to your racial or ethnic origin, religious beliefs, disability status, etc., to meet the local laws and regulations.

Sharing personal data with Third parties

- Where required or permitted by law, personal data may be provided to others, such as regulators and law enforcement agencies.
- From time to time, we may consider corporate transactions such as a merger, acquisition, reorganization, asset sale, or similar. In these instances, we may transfer or allow access to information to enable the assessment and undertaking of that transaction.
- We may use third parties to carry out certain activities (such as payroll processing, external audits, etc.), to help run our business and provide you benefits (such as pension plan or health insurance schemes), to facilitate your corporate travel & expenses and to carry out background verification.
- We share information with our internal staff and our group of companies for business and administrative purposes.
- Where required for your role, your business contact details may be shared with our clients, contractors, and suppliers.
- We may also share your CV's and background verification status to customers, upon request, to comply with our contractual obligations.

-

Existence of Automated Profiling and Decision Making

We do not use automated profiling do not carry out any processing activities that involve automated decisions.

For Further Details

For more information, such as your rights in respect of your personal data, transfer of personal data, data retention and security measures implemented by Virtusa, please *click here*.

THANK YOU