Annex 3: Definitions

October 2023

accenture

Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Accenture has entities and affiliates worldwide. Entities which sign up to the Processor BCR are referred to as 'Participating Entities'.

Accenture Security Operations Center (ASOC)

ASOC is where Accenture Employees report any information security incidents or breaches, and any physical or personal security emergencies. It can be reached 24 hours, every day of the year, and is for internal reporting purposes only.

Anonymization

Anonymization is permanently removing identifiable information from data so that the information can no longer be used to identify an individual. The process is irreversible. True anonymization is quite difficult to achieve.

Applicable Data Privacy Laws

means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data in the country in which the data exporter is established.

Anonymous, pseudonymised or aggregated data

Anonymous, pseudonymized or aggregated data are different ways to remove identifiers from personal data.

Chief Compliance Officer

Person ultimately responsible for overseeing our ethics and compliance program within Accenture.

Chief Information Security Officer (CISO)

The Chief Information Security Officer is responsible for leading Accenture's information security program.

Client

For the purposes of these Processor BCR, a Client is an entity not part of the Accenture group – usually a Data Controller - upon whose behalf Accenture processes certain Personal Data.

Client Data Protection (CDP) Program

ISO-certified program implemented by Accenture to establish and assess controls and standards, which provides engagement teams with a standardized approach to implement comprehensive and consistent security measures to help reduce business and financial risk to our Clients, their clients, customers and employees, and Accenture.

Client Personal Data

For the purposes of the Processor BCR, Client Personal Data is any Personal Data we process on behalf of Clients (Data Controllers) in our capacity as a Data Processor.

Code of Business Ethics (COBE)

Our COBE states that we operate with integrity and in an ethical manner. It is organized into six fundamental behaviors addressing issues such as how we should comply with laws, protect our people and the information we process and behave in a responsible manner as a corporate citizen. It applies to all Employees and people acting on our behalf such as contractors, suppliers and vendors. A copy is available **here.**

Controller Binding Corporate Rules (Controller BCR)

Controller BCR are a European Union mechanism to implement, in a legally binding manner, a level of Personal Data protection substantially equivalent to EU Data Privacy Laws protection standards, which is a prerequisite for many Cross Border Transfers of Personal Data. Accenture maintains Controller BCR (which were approved by EU Supervisory Authorities) throughout its worldwide organization. The Controller BCR apply to Personal Data processed by Accenture as a Data Controller and do not apply to Client Personal Data.

Cross Border Transfers

The activity of moving Personal Data from one country to another or making it accessible from abroad. Often, Applicable Privacy Laws place certain restrictions on such transfers, most notably the requirement to ensure ongoing protection of Personal Data, both for internal transfers within a corporate group and external transfers. EU Data Privacy Laws for instance, recognize, among others, EU Standard Contractual Clauses or BCR as frameworks to protect the Personal Data, unless exemptions apply.

Data Controller

The Data Controller is the entity that determines the purposes and means for processing Personal Data. A Data Controller definition is specific to EU Data Privacy Laws but is also used in several other, but not all, Local Privacy Laws. Accenture is considered the Data Controller, for example, in relation to Employees' Personal Data used for employment purposes. When providing services to a Client, Accenture is in most cases considered the Data Processor, the Client is the Data Controller and provides instructions for processing personal data on its behalf. It is possible to have joint data controllers determining the purposes and means of the processing.

Data Privacy Administrator

The lead Accenture Participating Entity for the purposes of the Processor BCR Intercompany Agreement – Accenture Privacy Agreement. Accenture has appointed a specific entity (Accenture Global Holdings Limited) based in the EEA as Accenture's Data Privacy Administrator to act on behalf of all Accenture Participating Entities (EEA/non-EEA) for the purposes of the Processor BCR.

Accenture Global Holdings Limited is a company incorporated in Ireland under company number 591684, whose registered address is at 1 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland.

Data Privacy Guidance

Documents and other information that are accessible to our Employees to help them comply with Accenture's BCR, its wider data privacy program and Applicable Data Privacy Laws, available at our internal data privacy website.

Data Privacy & Information Security Leads

Data Privacy & Information Security Leads are responsible for managing data privacy matters within their Market Unit (MU). They also carry out tasks delegated by Accenture Data Protection Officer and act as the point of contact for the relevant data privacy Regulators. The Data Privacy & Information Security Leads are the first point of contact for local data privacy questions from Employees.

Data Privacy Officer (DPO)

A DPO is a role established in accordance with Applicable Data Privacy Laws to provide oversight over Personal Data processing activities and perform specific tasks as mandated by such laws. Accenture's Data Privacy Officer is responsible for reviewing and monitoring Accenture's data privacy compliance, supported by the Data Privacy Officer Network.

Data Privacy Officer Network

The Data Privacy Officer Network - which consists of the Data Privacy Officer, the supporting DP Center of Excellence and the Data Privacy & Information Security Leads - manages Applicable Data Privacy Laws compliance activities and provides guidance for data protection impact assessments, data privacy Regulatory notifications, requests and audits, and Applicable Data Privacy Laws reporting. The Data Privacy Officer Network is led by the Data Privacy Officer.

Data Privacy Policy (Accenture Policy 90)

The purpose of this policy is to set out the duties of Accenture and its Employees when processing Personal Data about individuals.

Data Privacy Team

The Data Privacy Team, led by the Senior Director, Global Data Privacy, is responsible for defining, managing, and overseeing the Accenture data privacy program. It supports Employees in managing Personal Data of our Employees, Clients and other stakeholders in accordance with Applicable Data Privacy Laws and regulations.

Data Processor

An organization contracted by a Data Controller that processes data on behalf of that data Controller. A Data Processor is a term specific to EU Data Privacy Laws and can be used in other Applicable Data Privacy Laws.

Employee

"Employee" or "Employees" refers to all Accenture employees, contractors and interns, regardless of entity, workforce or career track.

European Economic Area

The European Economic Area (EEA) includes the European Union countries and Iceland, Liechtenstein and Norway allowing them to be part of the EU's single market.

EU Data Privacy Laws

EU Data Privacy Laws is a generic way of grouping together the GPDR and European Union Member State privacy Laws.

European Union

The European Union ("EU") is comprised of countries known as Member States which govern common political, economic, social and security policies. A list of EU countries is available here.

Fines, penalties & criminal sanctions

Most Applicable Data Privacy Laws impose some form of penalties, fines and criminal sanctions. The severity of these varies from country to country and generally depends on the nature of the non-compliance and the adverse consequences for individuals.

General Counsel

Accenture's most senior lawyer who heads up the legal function within Accenture.

General Data Protection Regulation (GDPR)

The "General Data Protection Regulation" (Regulation (EU) 2016/679)

Geographic Compliance and Corporate Team

The Geographic Compliance and Corporate Team provides local legal advice and data privacy support in specific jurisdictions where Accenture has a presence.

Individual Rights

Some Applicable Data Privacy Laws such as the GDPR give individuals specific rights in relation to their Personal Data. As a Data Controller, Accenture must have processes in place to help individuals exercise these rights. While the rights differ according to countries, we have adopted the broadest definition of these rights and they are incorporated within our BCR.

Intercompany Agreement - Accenture Privacy Agreement

Intercompany agreements are contractual arrangements between two entities which are owned by the same company. They can govern a number of different arrangements between entities for purposes such as services, transfer of goods and data handling arrangements. Accenture has put in place intercompany agreements, such as the Accenture Privacy Agreement as part of its BCR and international transfer arrangements.

Local Laws

Any statute, decision, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding requirements existing in the country where such applies.

Participating Entity

An Accenture entity that signs the Intercompany Agreement -_Accenture Privacy Agreement and is bound by the terms of the Processor BCR in relation to all their processing activities in scope of the Processor BCR, regardless of whether they act as data exporters or importers.

Personal Data

Personal Data, or PII ("Personally Identifiable Information") is information relating to an individual who is identified or directly or indirectly identifiable. Different Applicable Data Privacy Laws have different definitions, but typical examples include employee names or email addresses, vendor and client contact details and recruitment and alumni data.

Personal Data Breach

Personal Data Breaches are defined in a number of different laws (not just data privacy laws) and the elements usually relate to a number of categories of data, including Personal Data. Within EU Data Privacy Laws, 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.

Privacy by Default

Privacy by Default means implementing appropriate technical and organizational measures to ensure that privacy becomes the default option for processing Personal Data.

Privacy by Design

Privacy by Design means integrating privacy as a design component from the start when developing, designing, selecting and using applications, services and products which process Personal Data. Privacy should not be an afterthought or last-minute addition. It is a legal requirement under EU Data Privacy Laws and in other countries with Applicable Data Privacy Laws and is generally considered good practice.

Processing

Processing as defined in EU Data Privacy Laws is an all-encompassing term to describe anything which involves Personal Data, for example, viewing, access, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, use, disclosure, transmission, dissemination, alignment or combination, restriction, erasure or destruction.

Pseudonymization or 'key coding'

Strips away the identifiable information from specific data, replacing it with a non-identifiable pseudonym. An individual can no longer be identified from the

pseudonymized data alone without linking that data to additional information. The additional information necessary to return the data to an identifiable state would be held separately and securely elsewhere, to prevent re-identification.

Regulator

Most countries with Applicable Data Privacy Laws usually appoint a Regulator, with delegated responsibility for supervising data privacy in that country. They are referred to differently, depending on region but are commonly known as data protection authorities or agencies, supervisory authorities, privacy or information commissioners.

Senior Director, Global Data Privacy

The Senior Director, Global Data Privacy leads Accenture's Data Privacy program within Accenture Ethics & Compliance.

Sensitive Personal Data

The definition of Sensitive Personal Data varies by country but can include:

Ethnic or racial origin, political opinions, religious or other similar (philosophical) beliefs, trade union and similar memberships, physical/mental health or disability details (including pregnancy or maternity information), gender identity or expression, sexual orientation, biometrics and genetics data, criminal or civil offenses; geo location data, communications data, financial data, government, social security and similar IDs.

Sales and Delivery Legal Team

The team which advises, shapes, negotiates and manages Client contracts for Accenture's services, strategic offerings and go-to-market initiatives.

Sub processor

A sub processor is a third - party entity engaged by a Data Processor for the provision of services to Clients (Data Controllers). Sub processors can be entities from within Accenture or external entities.

Supervisory Authority

The Supervisory Authority is a term used to describe a data privacy Regulator with delegated responsibility for supervising data privacy in a particular country. European Union Member States generally refer to their data privacy Regulators as Supervisory Authorities.