Accenture Binding Corporate Rules (Controller BCR)

November 2026

Accenture Binding Corporate Rules (Controller BCR)

EXECUTIVE SUMMARY

INTRODUCTION

Complying with data privacy laws is part of Accenture group's Codes of Business Ethics (COBE) (e.g., the Accenture Code of Business Ethics and Avanade Code of Business Ethics). In line with our COBE, we implement recognized standards or legal arrangements, such as Binding Corporate Rules (BCR) within our business practices.

Accenture's Controller BCR (BCR-C) has been in place since 2009, following an approval process conducted by the European Union data privacy Regulators. The BCR-C was updated in 2018 to reflect new requirements under the EU General Data Protection Regulation. Accenture regularly adds new entities to the BCR-C and considers relevant legal changes to assess how they affect our BCR-C. This will often result in minor changes.

SCOPE

This document defines obligations Accenture has with regards to data processing in scope of the BCR -C and explains how we comply with those responsibilities across Participating Entities through our global data privacy program by addressing ethical aspects and legal compliance, accountability, opportunities, and risk.

Our BCR - C apply to all personal data processed by Accenture Participating Entities as a Data Controller or Data Processor for our own purposes. It does not apply to Accenture entities acting as a Data Processor for services we provide to clients.

The BCR-C does not override any Applicable Data Privacy Laws and regulations in countries where we operate. Accenture maintains safeguards mechanisms to protect data subjects' rights, according to the BCR-C.

ACCENTURE'S BCR-C COMMITMENTS

Accenture's data privacy obligations under the BCR-C are defined as a set of Commitments which establish our data privacy responsibilities and safeguards in relation to key requirements such as fair and lawful processing, data

Unrestricted **Copyright © 2026 Accenture. All rights reserved.**

minimization, security, and retention. The associated Annexes provide information on how we uphold these Commitments. In particular, Annex 1 explains our compliance measures including privacy by design and data protection impact assessments and how we cooperate with the supervisory authorities.

The table in Annex 2 sets out (i) information about the categories of individuals, (ii) the categories of personal data we may process about them; and (iii) a description of the purposes for which we process personal information.

A key component of the BCR-C is the data privacy rights given to individuals in relation to their personal information. These rights are explained in section Four of the Commitments. Annex 3 of the BCR-C sets out the process for individuals to exercise their rights, the procedure Accenture follows to facilitate these rights and the process for individuals to make data privacy complaints as well as how they can contact Accenture.

HOW IS THE BCR-C BINDING?

Accenture's BCR-C is made binding on all Participating Entities using an Intercompany Agreement called the Accenture Privacy Agreement (APA). All Accenture Participating Entities and their employees are bound by the BCR-C, irrespective of geographic location, and abide by the same internal rules for processing personal data. It also means that individuals' rights stay the same no matter where individuals' personal data is processed by Accenture.

MANAGING THE BCR-C

Annex 1 provides an overview of how Accenture manages its BCR-C. Day to day responsibility for managing the BCR-C lies with the Global Data Privacy team. Other Accenture functions have responsibility for matters such as auditing and security.

If you have any queries about the BCR-C, please direct them to Accenture's Data Privacy Officer: DataPrivacyOfficer@accenture.com

Unrestricted **Copyright © 2026 Accenture. All rights reserved.**

Unrestricted Copyright © 2026 Accenture. All rights reserved.

Table of Contents

Introduction....6
Purpose....6
Legal background....6

Accenture's BCR-C....6

Applicability and scope....7
Applicability....7
Scope....7
Accenture entities and affiliates....8
Categories of individuals, categories of personal data and processing, purposes, recipients, countries....8

Accenture's BCR-C commitments....8

One - Being ethical: Processing personal data ethically including in a manner consistent with our Code of Business Ethics (COBE)....9

Two - Being lawful: Defining purposes and limiting use of personal data to those purposes....9

Three - Being fair and transparent: Providing Notice, Consent and Choice 10
Collecting Information Indirectly....11
Using personal data for new purposes....11
Exceptions when collecting personal data indirectly....11

Four - Respecting Individuals' Rights....11
The right to be informed....11
The right to access their personal data processed by Accenture....12
The right to rectification....13
The right to erasure (also known as the 'right to be forgotten')....13
The right to restrict processing....14
The right to data portability....14
The right to object....15
Rights in relation to automated decision making and profiling....15
Rights in relation to making complaints with supervisory authorities and bringing court actions....16

Five - Following the rules on processing sensitive data....16

Six - How we minimize data collection, keep data accurate, up to date and follow retention schedules....17

Seven - Protecting personal data....18
General arrangements....18

Measures to control access....18
Personal Data breaches....18
Arrangements with vendors, suppliers and other third parties....19

Eight - Ensuring compliance with cross-border transfer requirements....20

Nine - Accenture's compliance with its BCR-C....21

Consequences of Non-Compliance....21

Publication of the BCR-C....21

Contact Information....21

Annex 1: How Accenture complies with its BCR-C Commitments....22

Preamble....22

Managing Data Privacy and Information Security....22

Managing the BCR-C....23

Cooperating with the Supervisory Authorities....23
General Cooperation procedures....23
Reporting matters to the Competent Supervisory Authority....23

How Accenture supervises data privacy compliance....24
Accountability....24
Training....25
Record keeping and evidence....25
Compliance with local laws....25
Privacy by Design - Building privacy into our projects, tools and applications....26
Privacy by Default....26
Privacy Reviews, Transfer Impact Assessments and Data Protection Impact Assessments....26
Audits....28
Liability....29

Employee violations of these BCR-C, Accenture policies or procedures and raising concerns....30

Annex 2: Categories of individuals, categories of personal data and processing, purposes, recipients, countries....30
Type....31
Explanation....31
Categories of individuals....31

Annex 3: Individuals Rights Requests and Complaint Handling Procedure 37

Table of Contents....37

1. Purpose....38

2. Who handles IRRs and Complaints?....38

3. Making a request....38

4. Submitting a request....38
4.1. What is a request?....38
4.2. What do individuals need to know?....39

5. How Accenture manages a request....40
5.1. Assigning Case Owners....40
5.2. Request management....40
5.3. Additional Considerations....42

6. Escalation options....42

7. How does Accenture manage complaints?....43

8. Record Keeping, reports and further action....43

Annex 4: Definitions....44

Annex 5: Accenture Intercompany Agreement – Accenture Privacy Agreement....44

Annex 6: Supporting Documentation and Resources....44
General:....45
Policies & Standards:....45
Internal Guidelines and Global Templates....46

Annex 7: Revision History....46

Introduction

Purpose

The purpose of this document is to:

- explain Accenture's data privacy obligations and commitments;
- define Accenture employees' responsibilities and accountability for data privacy;
- describe individuals' rights under the Binding Corporate Rules (BCR-C);
- explain how Accenture handles complaints and/or queries relating to personal data processing;
- provide information on how to contact Accenture regarding data privacy.

Legal background

Data privacy laws govern how Accenture handles personal data in many of the countries where we operate. Those laws define our legal status and obligations. Where Accenture determines the purpose, means and conditions of processing personal data, we are a decision maker, generally referred to as a "data controller." Where we act as a service provider on behalf of others – typically our clients – we are a "data processor".

There are strict European Data Privacy Laws on transferring personal data outside the European Economic Area (EEA) to another country. These laws apply to all transfers of personal data outside the EEA, including internal transfers of data within a group of companies. Such transfers are generally only allowed if a substantially equivalent level of protection has been put in place using mechanisms which have been approved by European Regulators unless certain exemptions apply.

Accenture's BCR-C

To comply with these European requirements, Accenture has implemented a set of data privacy rules known as Binding Corporate Rules (BCR). These are legally binding, and Accenture must integrate the requirements within our operation practices.

They are made up of:

a) a set of the BCR-C Commitments and associated *Annexes:*

- Annex 1: *How Accenture complies with its BCR-C;*
- Annex 2: *Categories of individuals, categories of personal data, processing, purposes recipients, countries;*
- Annex 3: *Individual rights requests and complaint handling procedure;*
- Annex 4: *Definitions;*

- Annex 5*: Intercompany Agreement-(Accenture Privacy Agreement),* which sets out Accenture's data privacy obligations, the safeguards we have established to meet those obligations, how we manage individuals' rights and complaints under the BCR-C and how to contact us.

b) they are supported by a set of supplementary documents which are not formally part of the BCR-C:

- Annex 6: *Accenture Supporting Documentation;*
- Annex 7: *Revision History.*

The BCR-C reflect the standards contained in European Data Privacy Laws and the BCR-C have been approved by most data privacy Regulators in Europe. Having the BCR-C means that all our group entities which sign up to it must comply with the same internal set of rules – that there are appropriate and uniform data privacy safeguards in place across our organization. It also means that individuals' rights stay the same no matter where individuals' personal data is processed by Accenture.

Accenture has a global data privacy program to manage these commitments and to address ethical and legal compliance, accountability, opportunities and risk. All Accenture Participating Entities and employees bound by these BCR-C, irrespective of geographic location, abide by the same rules for processing personal data.

You can find an explanation of the data privacy terms used in this document in Annex 4, Definitions.

Applicability and scope

Applicability

Accenture's BCR-C apply to all personal data processed by Accenture Participating Entities as a Data Controller for our own purposes such as recruitment, employment or marketing. We process personal data about a wide range of individuals including graduates, potential recruits, employees, alumni, prospective and existing clients, contacts, children, and adolescents (see Annex 2 for more information about purposes and categories of individuals).

The BCR -C Commitments:

a) require all Accenture Participating Entities and employees who collect, use and store personal data to understand the rules and their responsibilities when processing personal data;

b) require all Accenture employees to understand how to respect and manage individuals' rights in relation to their data; and

c) govern the circumstances in which one Accenture entity processes personal data on behalf of another Accenture entity

Scope

Please note that these BCR-C apply to Accenture as a Data Controller transferring data point out in Annex 2. It does not apply to Accenture as a Data Processor for services we provide to clients. For client-provided personal data, Accenture has a Client Data Protection (CDP) program with separate policies and procedures to implement data privacy requirements applicable to client-owned data. There is a dedicated CDP team responsible for providing guidance and controls.

This document is without prejudice and does not override any Applicable Data Privacy Laws and regulations in countries where we operate. Note where the Local Law requires a higher level of protection for personal data it will take precedence over the BCRs. Accenture maintains safeguard mechanisms to protect data subjects' rights, according to the BCR-C.

Accenture entities and affiliates

Accenture has offices and operations throughout the world. Personal data may be transferred or be accessible throughout Accenture's global business and between its entities and affiliates. For a full list of our entities which are signed up to the BCR-C and their locations, click here.

Categories of individuals, categories of personal data and processing, purposes, recipients, countries

The table in Annex 2 sets out information about (i) the categories of individuals, (ii) the categories of personal data we may process about them; and (iii) a description of the purposes for which we process personal information. Our data privacy notices and data privacy statements are where we provide specific information to individuals, for example, our privacy statement on the accenture.com site.

Accenture's BCR-C commitments

To protect personal data, Accenture and our employees comply with these commitments which are appropriately reflected in our core Data Privacy Policy (known as Policy 90), procedures, controls and guidance. Accenture's BCR-C Participating Entities and employees who access, collect, delete, retrieve, store, or otherwise use personal data for any purpose, are "processing" that data and are responsible for understanding how data privacy impacts their role and their use of personal data using the data privacy resources Accenture provides.

One - Being ethical: Processing personal data ethically including in a manner consistent with our Code of Business Ethics (COBE)

It is our employees' overarching responsibility to be ethical and comply with data privacy laws by complying with these BCR-C Commitments, the applicable Data Privacy Policy, (any related policies, procedures and guidance) and by acting with integrity and processing personal data in a way which is consistent with Accenture's core values and COBE.

Two - Being lawful: Defining purposes and limiting use of personal data to those purposes

Accenture processes personal data for specified and lawful purposes which are clearly explained to individuals when we process their data. Lawful Processing means that Accenture will not process personal data, unless one of the following conditions applies:

(i) the individual concerned has consented to the processing;

(ii) Accenture processes the data to:

(1) perform, or take steps with a view to enter into, a contract with the individual concerned;

(2) comply with a legal obligation which Accenture is subject to;

(3) protect the vital interests of individuals in a `life or death' situation; or

(4) perform a task in the public interest or to exercise official authority;

(iii) Accenture needs to carry out such processing to pursue Accenture's Legitimate Interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual concerned; or

(iv) in circumstances permitted by Applicable Data Privacy Laws.

Accenture will not use personal data for new purposes without following our internal procedures to verify that such processing can take place lawfully by taking the following into account:

(i) links between the current purposes and the further respective processing purposes;
(ii) the context of the original data collection, with a particular focus on the relationship between Accenture and individuals;
(iii) the nature of the personal data, in particular, if the data in question is sensitive personal data;
(iv) possible consequences for individuals if their data are processed further; and

(v) appropriate safeguards which may include encryption or pseudonymization.

Three - Being fair and transparent: Providing Notice, Consent and Choice

Accenture provides individuals with information (for example, in a data privacy notice or privacy statement) to explain how their data will be processed by Accenture to ensure fair and lawful processing. The information is made easily accessible to individuals and is provided in a clear, transparent manner using plain and intelligible language.

The information Accenture provides

An individual has the right to know about Accenture's processing of their personal data and to verify whether that processing is lawful. The information Accenture will provide to individuals shall include the following:

a) the name of the relevant Data Controller and their contact details;

b) the contact details of the Data Privacy Officer or designated data privacy contact;

c) the purposes for which we intend to use such data including the legal basis for processing the data (where we have relied on the legal basis, we will explain what that legal basis is);

d) the recipients or categories of recipients of the data;

e) any relevant information about international transfers of the data, in particular; the existence/absence of an adequacy decision/safeguards in place and where to obtain a copy of a relevant decision, if available;

f) the retention period and/or any relevant retention criteria;

g) information about the individuals' rights (e.g., access, rectification, erasure, restriction, objection and portability);

h) information about any automated decisions/profiling including the logic involved and significance of such processing for the individual;

i) the individual's right to withdraw consent, if applicable;

j) the right to lodge a complaint with the supervisory authority;

k) the consequences of failing to supply data where the processes relate to a statutory or contractual requirement; and

l) any additional information Accenture deems necessary to process the data fairly and lawfully.

Where Accenture has already provided this information, we will not continually provide it as part of each subsequent interaction with the individual, unless failure to do so would infringe these rights.

Collecting Information Indirectly

Where collecting personal data about an individual indirectly (for example, from a publicly available source), Accenture will inform the individual that Accenture is holding the data and what it intends to do with the data after obtaining it. Accenture will also provide individuals with any additional information necessary to process the data fairly, transparently and lawfully. This information will include the categories specified above (Commitment 3 a-l).

Accenture will provide this information as part of the initial communication with the individual or where a disclosure is being made to another recipient before or when the first disclosure is made, but at the latest within one month of obtaining the data.

Using personal data for new purposes

Accenture will make sure that information to individuals is also provided where existing personal data is going to be used in a new way, or for incompatible purposes prior to the commencement of such processing.

Exceptions when collecting personal data indirectly

When we collect information indirectly, there are some exceptions. The information referred to in Commitment 3 categories a-l will not be provided to the individual by Accenture, if:

a) the individual already has the information; or

b) the effort involved would be disproportionate; or

c) there are laws or professional secrecy obligations which Accenture is subject to which require obtaining or disclosing the data or that require the data and information about the data, remain confidential.

In determining what does or does not constitute a 'disproportionate effort,' Accenture will balance the amount of effort required against the amount, if any, of a prejudicial effect to the individual if such information was not provided to them.

Four - Respecting Individuals' Rights

Individuals have rights in relation to their personal data processed by Accenture. We respect these rights and have processes in place to recognize and respond to individuals wishing to exercise these rights. Our employees have guidance to follow when handling individuals' rights requests. The rights include:

The right to be informed

This right has been covered in detail above [See Three - Being fair and transparent].

The right to access their personal data processed by Accenture

1. An individual has the right to request access to the personal data we process about them. When Accenture receives such a request, we will first take reasonable steps to:
    a. identify the individual making the request;
    b. decide whether Accenture is processing their personal data; and
    c. ask for specific information to help locate that data.
2. Accenture will provide the individual with the following information:
    a. whether data is held and if so, the relevant purpose, together with an indication of the source[s] of the data if known;
    b. the categories of personal data;
    c. the recipients of the data, including recipients located in other countries and details of the appropriate safeguards in place for the transfer of their data to other countries;
    d. any automated decision-making or profiling applied to the personal data and the significance of such processing;
    e. how long the data will be retained or the retention criteria;

    Accenture will also make the individuals aware of their rights to request rectification, erasure, restrictions on use of the data by Accenture or the right to object and their right to lodge a complaint with a supervisory authority.
3. Accenture will provide a copy of this information within one month of receiving an individual's request, or within any specific period (if one month or less but no more than one month) that may be required by Local Law in any country. Accenture will generally provide the information in a commonly used electronic format unless there is a compelling reason to provide it in another format.
4. Accenture may, however, refuse to provide an individual with information where disclosure of that information would reveal information about another individual (in which case, Accenture will provide as much of the information as possible without revealing information about the other individual). Accenture may decide that it is reasonable to provide the information without the other individual's agreement or may decide, given the circumstances, to obtain the consent of the individual to release the information. In addition, in some countries localized guidance may provide other legitimate reasons which we would need to take into consideration, for refusing an individual's request for access, in accordance with local law.
5. Where Accenture refuses to comply with a request, we will explain our reasons for doing so to the individual and inform them of their right to

complain to a supervisory authority and/or seek judicial remedy within one month of receiving our refusal to comply with the request.

The right to rectification

An individual may request that Accenture rectify their personal data if the data is inaccurate or incomplete.

a) If Accenture has disclosed the data to a recipient, we will inform the recipient of the request where feasible to do so. An individual may request information about the recipients from Accenture.

b) If Accenture agrees that the data is incorrect or incomplete, we will delete, correct or amend the data.

c) If we do not agree that the data is incorrect or incomplete, Accenture will inform the individual and explain their right to complain to a supervisory authority and to seek judicial remedy.

d) Accenture will keep a record that the individual considers the data to be inaccurate or incomplete.

The right to erasure (also known as the ‘right to be forgotten’)

Accenture will abide by a request from an individual to erase their personal data under the following conditions as specified within privacy laws:

a) the personal data is no longer necessary for the purpose for which they were collected or otherwise processed; or

b) an individual withdraws consent and there are no other legal grounds for processing; or

c) an individual objects to the processing and we have no overriding Legitimate Interests for continuing to process their data; or

d) the personal data is being unlawfully processed; or

e) the data must be erased to comply with a legal obligation applicable to Accenture as a data controller; or

f) the personal data is processed in relation to the offer of information society services to a child.

There are circumstances when Accenture can refuse an erasure request; these include:

a) exercising the right of freedom of expression and information;

b) complying with a legal obligation applicable to Accenture as a data controller or for the performance of a public interest task or exercise of official authority;

c) for public health reasons or for purposes in the public interest;

d) for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or

e) for the establishment, exercise or defence of legal claims.

Accenture will inform any recipients about the erasure request unless this would require a disproportionate effort. Where Accenture has made the data public, it will take reasonable steps, (taking into account cost and technology), to inform other recipients of the data to erase links to, copies or replication of those personal data.

Accenture will comply with any legally specified timeframes within data privacy laws for complying with such requests.

The right to restrict processing

Accenture will agree to restrict processing of an individual's data if one of the following applies:

a) When an individual contests the accuracy of the data, Accenture will restrict using the data until the accuracy can be verified;

b) The processing is unlawful and the individual requests a restriction of use rather than erasure of their data;

c) Accenture no longer needs to process the personal data, but the individual requires the data to establish, exercise or defend a legal claim; or

d) In circumstances where an individual has objected to the processing (which was necessary for purposes in the public interest or Accenture's Legitimate Interests) and Accenture is considering whether Accenture's interests override the interests of the individual.

If there is a restriction on processing, Accenture has the right to retain the data we will refrain from processing for unlawful purposes but may continue to use the data for legitimate purposes.

Accenture will inform any recipients of the personal data about the restriction unless it is disproportionate to do so. An individual can request information about the identity of the recipients from Accenture. If Accenture lifts the restriction on processing, the individual will be informed.

The right to data portability

An individual has the right to request portability of personal data which they provided to Accenture, if:

a) the processing is based on the individual's consent or for the performance of a contract, and

b) the processing is automated.

This right only applies to data an individual has provided to Accenture.

If the personal data includes data about other individuals, Accenture will take steps to ensure providing the information would not affect the rights and freedoms of other individuals.

Accenture will:

a) provide the information free of charge and in a structured, commonly used and machine-readable format,

b) transfer the information directly to another data controller at the request of the individual, where technically feasible,

c) respond to the request within one month,

d) notify the individual within one month of receiving the request if we cannot respond within one month, explaining the reasons for the delay,

e) respond within 2 months where a response has been delayed,

f) inform an individual within one month of receiving their request if we cannot respond to such a request and make them aware of their right to make a complaint to the supervisory authority and/or seek judicial review.

The right to object

An individual has the right to object (under certain circumstances) to processing of their data by Accenture. Accenture will abide by any valid request from an individual who objects to the processing of their data by Accenture.

Direct marketing objections – Accenture has systems and processes in place to record an individual's request not to use their data for direct marketing purposes and for profiling as it relates to direct marketing.

Objecting to scientific or historical purposes – Accenture has systems and processes in place to manage an individual's request to object to their data being used for scientific research, historical research or statistical purposes.

Under certain circumstances, there may be grounds for Accenture to continue certain types of processing where we can demonstrate that our Legitimate Interests override the rights of an individual or in instances where the processing is necessary for the establishment, exercise or defense of legal claims.

Accenture will respond to an individual's request within the specified timeframe. Where we cannot process an objection, a notification explaining the reasons why will be sent.

Rights in relation to automated decision making and profiling

An automated decision is when a decision is made about an individual using technology specifically designed for decision-making purposes. This includes profiling individuals. Under some data privacy laws, such as the General Data Protection Regulation (GDPR), an individual has the right not to be subjected to solely automated decisions which produce legal effects or otherwise similarly significantly affect them. An individual has the right to ask for a review of the decision, offer their opinion and challenge the decision.

The right does not apply, where the decision is:

- made with the explicit consent of an individual;
- for the purposes of a contract; or

- authorized by law.

Where consent or contracts are relied on, there must be suitable safeguards (like human intervention) to review the decision, in order to protect the individual. There are restrictions on making automated decisions using sensitive personal data and children's data.

Accenture will comply with the relevant requirements when making automated decisions and will institute any additional safeguards to protect individuals' rights where required to do so.

Rights in relation to making complaints with supervisory authorities and bringing court actions

Individuals have the right to come directly to Accenture for resolution of their complaint, to register a complaint directly with the relevant supervisory authority - this is a choice between the supervisory authority in the EU Member State where the individual habitually resides, their place of work or place of the alleged infringement. Individuals, who can be represented by a not-for-profit body, organization or association under the conditions set out in the GDPR or Local Laws, also have the right to make a claim against Accenture before the competent court of the EU Member State where they habitually reside or where Accenture has an establishment. We encourage and welcome individuals to come to Accenture first to seek resolution of any complaint. For more information on our complaint handling procedure, review Annex 3 or to find a full list of Member State supervisory authorities please click here.

Five - Following the rules on processing sensitive data

Certain categories of personal data referred to as "sensitive" or "special" are subject to additional legal requirements because they carry higher risks for an individual if misused or processed incorrectly. The definition of sensitive 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.

Where Accenture collects these types of data we will only do so, if:

(i) the individual concerned has given their explicit consent that we may do so, based on a full understanding of why the data is being collected, or

(ii) Accenture needs to do so to meet our obligations or exercise our rights under employment, social security and social protection law, or

(iii) in exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned, or

(iv) the processing relates to personal data which are manifestly made public by the individual, or

(v) the processing is necessary for the establishment, exercise or defence of legal claims, or

(vi) the processing is for reasons of substantial public interest, or

(vii) it is necessary to process the data for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health/social care systems and services mandated by law or in relation to a contract with a health professional subject to suitable safeguards, or

(viii) in circumstances permitted by Applicable Data Privacy Laws.

Accenture will not use personal data, including sensitive personal data, for new purposes without following our internal procedures to verify that such processing can take place lawfully.

Accenture will always treat any collection, use or storage of sensitive data with more scrutiny as such data requires additional privacy, legal and security safeguards. Accenture will not process sensitive data without following our internal procedures to verify that such processing can take place. These procedures include conducting a Privacy Review and Data Protection Impact Assessment (DPIA), when required, and following any recommendations to institute additional protective measures for sensitive data recommended by our internal data privacy and security teams. Accenture will consult with the Competent Supervisory Authority, where required to do so.

Accenture may in exceptional circumstances, rely on consent given on behalf of the individual, for example, by a company employee or on behalf of a family member or dependent where this is permitted by law. In these circumstances and where relevant to do so, Accenture will provide sufficient information for the employee to provide to family members.

Six - How we minimize data collection, keep data accurate, up to date and follow retention schedules

Accenture has procedures in place to only collect personal data that is relevant and reasonably required to achieve a specific purpose. Where feasible and appropriate, we consider using anonymous, pseudonymized or aggregated data instead of personal data.

Accenture has controls, procedures and systems to verify that personal data is accurate, up to date and relevant to achieve a specific purpose. Relevant guidance is made available to our employees for amending data, which is inaccurate, when required.

Accenture does not retain personal data for longer than necessary. We maintain specific records management and retention policies and procedures, so that personal data are deleted after a reasonable time according to the purposes they were obtained, or in accordance with legal/regulatory specified retention requirements.

When Accenture no longer needs to retain, there are procedures for the secure disposal of personal data.

Seven - Protecting personal data

General arrangements

Accenture maintains organizational, physical and technical security arrangements for all the personal data it holds. Accenture has protocols, controls and relevant policies, procedures and guidance to maintain these arrangements, taking into account the risks associated with the categories of personal data and the processing we undertake.

Measures to control access

There are protocols in place to prevent unauthorized access and where appropriate, we have access control procedures to limit access to personal data; to authorized individuals. Where relevant, we observe restrictions on disclosures applicable under relevant laws, contractual arrangements or relevant to Accenture's processing; including when we share data with vendors, suppliers and partner organizations.

Personal Data breaches

Accenture has policies, procedures, and protocols in place for managing and responding to personal data breaches, understood as 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. All instances of suspected or known breaches where there may have been inappropriate access to, or an unauthorized disclosure of personal data must be reported immediately to the appropriate Accenture or Avanade Security Operations Center [ASOC]. All employees are required to follow our security instructions. As part of our incident response processes there are procedures for informing senior management, our Senior Director Global Data Privacy, Data Privacy Officer (DPO), other BCR-C Participating Entities affected by the incident and relevant members of the Global Data Privacy team of the incident and where required, notifying the supervisory authorities without undue delay, and, where feasible, not later than 72 hours after having become aware of the personal data breach. In addition, where required, we will notify individuals without undue delay where the breach is likely to cause significant risks to the rights and freedoms of individuals. There are also procedures for notifying other relevant bodies about breaches when legally required to do so in certain jurisdictions or when Accenture considers it appropriate.

Accenture maintains a record of personal data breaches which includes details about the breach incident, the effects (if any) on individuals, Accenture or any

other party, and remedial action necessary to resolve the breach. Accenture will make these records available to the relevant supervisory authority.

Arrangements with vendors, suppliers and other third parties

Accenture recognizes that adequate security is important where it arranges for outside service providers (also known as “data processors”) to process personal data on our behalf. Accenture entities, as the data controllers, will enter into contractual arrangements with all our service providers that process personal data on our behalf, in compliance with any specific processor obligations, relevant security provisions and requirements as per any Applicable Data Privacy Laws. This includes situations when one Accenture entity processes personal data on behalf of another Accenture entity.

These contractual arrangements will include:

(i) a requirement to process personal data based solely on the instructions of the Accenture entity which is the Data Controller;

(ii) the rights and obligations of the Data Controller;

(iii) the scope of processing (duration, nature, purpose and the categories of personal data);

(iv) an obligation on the Data Processor (and where relevant, Data Sub-Processor) to:

a. implement appropriate technical and organizational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular, where the processing involves the transmission of data over a network, and against all other unlawful forms of processing and security requirements under the law;

b. provide full cooperation and assistance to the Accenture entity to allow individuals to exercise their rights under the BCR-C;

c. provide full cooperation to the Accenture entity so it can demonstrate its compliance obligations – this includes the right of audit and inspection;

d. make all reasonable efforts to maintain the personal data so that they are accurate and up to date, at all times;

e. return or delete the data at the request of the Accenture entity, unless required to retain some or part of the data to meet other legal obligations; and

f. maintain adequate confidentiality arrangements and not disclose the personal data to any person except as required or permitted by law or by any agreement between the Accenture entity and the Data Processor or with the Accenture entity’s written consent.

If service providers are located in countries outside the EU and they have access to or otherwise process personal data that relates to EU individuals or came from Accenture entities in the EU, the contracts with such service providers shall include the approved EU standard clauses (controller to processor) or shall be based on another EU-approved mechanism for allowing Data Transfers.

Eight - Ensuring compliance with cross-border transfer requirements

Data privacy laws place restrictions on transfers of personal data across borders for any type of processing (collection, access, use, storage, etc.). These restrictions also apply to internal transfers of personal data within Accenture across the countries where we operate, and to transfers of personal data to vendors, suppliers, partners or other third parties located in different countries.

Accenture has guidance in place to ensure that appropriate safeguards (including contractual arrangements where needed) are put in place for transfers of personal data to countries which do not have data protection laws or whose laws do not provide a level of protection which corresponds to the standards recognized by or offered within the EU. This guidance includes information on when to apply the correct safeguards and contractual arrangements before any such cross-border transfers take place. This includes assessments of third country laws and practices prior to the transfer taking place (including data in transit) in order to determine to what extent European Essential Guarantees are respected. The BCR-C Participating Entities may only use the BCR-C as a tool for transfer where this assessment has occurred.

If Accenture concludes that an adequate level of protection for personal data cannot be guaranteed in the third country concerned, the Data Exporter in a Member State, if needed with the help of the Data Importer, shall assess and define supplementary measures to ensure a level of protection which is essentially equivalent to that in the EU. Where effective supplementary measures could not be put in place, data importer is in breach or unable to comply with BCR-C, the transfer at stake will be suspended or ended. Transfers will be made if BCR members can deliver compliance.

The Data Importer should, at the choice of the Data Exporter, immediately return or delete the personal data, including its copies, transferred under the BCR-C where:

-compliance with BCR-C is not restored within one month of the suspension of the transfer by the Data Exporter, or

- the Data Importer is in persistent breach of the BCR-C, or

-the Data Importer fails to comply with a binding decision of a competent court or a Competent Supervisory Authority regarding its obligations under the BCR-C.

Under these circumstances, the Data Importer must continue to ensure full compliance with BCR-C until the personal data is either deleted or returned. If Local Laws applicable to the Data Importer prevent the return or deletion of the transferred data, the Data Importer must warrant that it will maintain compliance with BCR-C and limit the processing of the data strictly to the extent and duration required by those Local Laws.Accenture has a uniform approach towards the handling of personal data requests that are massive, disproportionate, and indiscriminate from public authorities directed to any Accenture entity by any public authority or body, whether such personal data relates to Accenture

employees, contractors, service providers, Accenture clients or their customers, for example according to local surveillance laws or regulations.

Accenture has put in place procedures for implementing these safeguards to cover our day-to-day processing, for example, via these BCR-C for internal transfers, or procurement contracts that include the relevant obligations conferred upon data processors or Data Sub- Processors as specified in privacy laws and other mechanisms. Our safeguards include sufficient protections to guard against any onward transfer of data to controllers or processors which are not part of the BCR-C.

Nine - Accenture's compliance with its BCR-C

(a) Accenture has internal arrangements to:

(i) facilitate and monitor compliance with our BCR-C Commitments, as described in Annex 1: How Accenture complies with its BCR-C Commitments;

(ii) allow individuals to effectively exercise their rights guaranteed under the BCR-C and consider and respond to complaints by individuals as described in Annex 3: Individuals' Rights Requests and Complaint Handling Procedures; and

(iii) cooperate and liaise with the supervisory authorities in relation to the BCR-C.

(b) All individuals may rely upon these procedures and/or exercise their rights provided for in the BCR-C by following the processes referred to in Annex 3 or by contacting the Accenture Data Privacy Officer, the Senior Director Global Data Privacy, the Global Data Privacy team, the local Data Privacy & Information Security Lead or the designated country contact.

(c) If an Accenture entity becomes aware of the existence of any requirements under Local Laws or other factors that would have a substantial adverse effect on our ability to comply with our BCR-C commitments (or would have such an effect even if the requirements were not imposed on the Accenture entity by law) it will inform the Global Data Privacy team and the Accenture entity (or entities) whose data we process and whose data is affected by such local laws.

Consequences of Non-Compliance

If Accenture fails to meet our data privacy obligations as a data controller and under the BCR-C, we may cause risks or harm to individuals resulting in fines, penalties, criminal sanctions, loss of business and adverse publicity. We therefore take compliance very seriously.

Publication of the BCR-C

The BCR-C is made available via the Accenture.com website and certain other websites of the group to external parties and internally via the corresponding Accenture entity's internal portal. Where we are required to publish the BCR-C in a local language, we will do so. Upon request, we will also e-mail an electronic PDF version of the BCR-C to an individual, without undue delay.

Contact Information

Questions relating to the BCR-C should be sent to the Global Data Privacy team – DataPrivacyOfficer@accenture.com.

Annex 1: How Accenture complies with its BCR-C Commitments

Preamble

The purpose of this Annex is to set out the rules and the procedures to be followed by all Accenture Participating Entities and employees to ensure compliance with the BCR-C Commitments. The BCR-C and this Annex do not apply to personal data processed by Accenture on behalf of and upon the instructions of clients of Accenture during the provision of client delivery services.

Managing Data Privacy and Information Security

Accenture has a Global Data Privacy Team led by the Senior Director, Global Data Privacy that defines, oversees, maintains and updates the data privacy program.

We also have a Data Privacy Officer (DPO) who reports to the Senior Director, Global Data Privacy, but also has the right to directly escalate issues to other highest management level, including board level, the Chief Compliance Officer and the General Counsel, i if any questions or problems arise during the performance of ones duties. Across the regions where we operate, we have a Data Privacy Officer Network (which includes Data Privacy & Information Security Leads) and Information Security Sponsors supported by the Geographic Compliance and Corporate team, Asset Stewards and designated individuals within corporate functions; each with specific responsibilities and accountability for data privacy management.

The responsibilities for different aspects of data privacy compliance and monitoring are shared across the team to oversee and ensure compliance with the BCR-C and Applicable Data Privacy Laws and regulations at global, regional and country level.

To help manage our information security program, Accenture has a global Information Security team led by our Chief Information Security Officer. Across our global organization we have a network of information security teams responsible for overseeing the use of technology to protect personal data, deploying risk management procedures to continually assess and monitor our information security risk position, managing Accenture’s cyber incident responses and managing the appropriate information security training and communications.

Accenture regularly reports (and where necessary, by exception) on information security and data privacy matters to our Board of Directors, Global Management Committee and Chief Compliance Officer and General Counsel.

Due to the global and complex nature of Accenture’s operations, there may always be more than one member of the team involved in routine reporting and

reporting on individual investigations and/or breaches. Monitoring, training and compliance efforts are all dealt with both globally and locally.

Questions relating to the BCR-C should be sent to the Global Data Privacy team – DataPrivacyOfficer@accenture.com.

Managing the BCR - C

Day-to-day responsibilities for managing the BCR-C sit with the Global Data Privacy team. This includes routine monitoring and reporting. Routine auditing of the BCR-C is managed separately by other functions such as our internal audit and compliance monitoring teams.

Collectively, their duties are to:

a) be responsible for maintaining the BCR-C up to date in order to reflect current situation and ensuring they are modified when required to do so to reflect regulatory changes, alterations to the Accenture group structure or any other changes which should be reflected within the BCR-C;
b) maintain a full list of the BCR members and ensure this list is up to date;
c) develop audit controls for the BCR-C;
d) monitor compliance with the BCR-C;
e) record and track all changes and updates to the BCR-C and the rationale for the updates and provide this information, as well as the updated list of BCR-C members to Accenture BCR-C entities or the Supervisory Authorities, without undue delay or as part of our annual notification;
f) communicate with the Competent Supervisory Authority and BCR-C entities, if a proposed change to the BCR-C either affects the level of protection offered by the BCR-C or significantly affects the BCR-C, in particular, its binding nature;
g) where a modification to the BCR-C would possibly be detrimental to the level of the protection offered by the BCR-C or, it must be communicated in advance to the Supervisory Authorities, via the BCR-C Lead, with a brief explanation of the reasons for the update;
h) communicate any other relevant matters to the Competent Supervisory Authority or other supervisory authorities where necessary;
i) ensure that the annual notification will happen even in instances where no changes have been made, and it will include the renewal of the confirmation regarding assets,
j) ensure that the BCR-C is up-to-date and in compliance with Article 47 GDPR and EDPB Recommendations;
k) provide the necessary information to data subjects, and, upon request to Competent Supervisory Authority.

Cooperating with the Supervisory Authorities

General Cooperation procedures

All Accenture entities have a duty to cooperate with the Supervisory Authorities (SAs) for information or inspection, including on-site, if necessary. Each Accenture entity will comply with their binding decisions or advice on any issues relating to the BCR-C, (any advice would be subject to legal review to consider any factors which inhibit the entity's ability to comply and where relevant, we

would discuss alternative legal remedies with the SAs), be willing to be audited by the SAs, if required, or provide audit results and reports, if asked to do so. No transfer will be made to an Accenture entity under the BCR-C until they have signed the APA and are effectively bound by the BCR-C. However, we may use other transfer mechanisms to facilitate transfers until they join the BCR-C. Changes to the BCR-C entity list will be reported to all Accenture entities signed up to the BCR-C and to the relevant Supervisory Authorities via the Competent Supervisory Authority.

Reporting matters to the Competent Supervisory Authority

Routine reporting: Accenture will report routine updates to the BCR-C along with an updated list of Accenture BCR-C Participating Entities as part of its annual update and in line with requirements specified in the section: Managing the BCR-C.

Conflicts between Local Laws and the BCR-C: Accenture has a duty to inform the supervisory authorities of any conflict between local law requirements and the BCR-C where this conflict would have a substantial adverse effect on the guarantees provided under the BCR. Accenture entities have a duty to report such conflicts to the Global Data Privacy team as soon as they become aware. This includes any legally binding requests for disclosure of personal data to a law enforcement or other security agency as explained directly below.

Disclosure and transfer requests: All Accenture entities agree that transfers of personal data to any public authority or body shall be limited to the minimum amount of information permissible under the request, and cannot be massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society.[1]

All Accenture entities must report any such disclosure requests and if they become aware of any direct access by public authorities to personal data transferred pursuant to the BCR in accordance with the laws of the country of destination to the Accenture Global Data Privacy team. The Global Data Privacy team will then inform, where possible, the data subject about the request, the identity of the requesting party the legal basis for the request and the response provided [unless we are prohibited or temporarily prevented from doing so under criminal law provisions specifying confidentiality during the course of a law enforcement investigation].

All Accenture entities must endeavor to have the prohibition on notification waived as soon as possible to provide the data subject with as much information as possible to be able to evidence their efforts to do so.

All Accenture entities acting as Data Importers shall review the legality of the requests and seek interim measures to suspend the request -if it is possible under the local procedural rules. All the documentation related to the requests must be

[1] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

available to the Accenture entity acting as data exporter and to the SA, upon request.

All Accenture entities must keep a record of these disclosure requests they receive for as long as the personal data concerned is subject to the BCR-C. These records should include details about the disclosure, the categories of data requested, the identity of the requestor [unless prohibited by law to retain this information] and any other relevant information.

How Accenture supervises data privacy compliance

Accountability

Everyone who works for or on behalf of Accenture is:

(i) responsible and accountable for processing personal data ethically and lawfully;

(ii) expected to comply with Accenture's policies and Data Privacy Guidance when processing personal data; and

(iii) expected to understand the data privacy requirements which have relevance to the personal data they process on behalf of Accenture using our policies, guidance and training material.

Accenture also has processes and procedures in place to manage and monitor our compliance with data privacy requirements. We have appropriate technical and organizational measures to meet these requirements. Everyone at Accenture is expected to follow our processes and comply with our procedures and measures.

Training

Accenture maintains a data privacy training program for all our employees. The program is constantly available for employees. In addition, all Accenture employees who regularly process personal data, who are involved in the collection of personal data or in the development of tools used to process personal data will be given appropriate and anually data privacy training, including up to date BCR-C training, and how to manage requests for access to personal data by public authorities. If required to do so, Accenture will provide the supervisory authorities with examples of our training program.

Record keeping and evidence

Accenture maintains electronic records and evidence of our data processing activities and compliance, in the event that we need to show individuals, auditors, supervisory authorities, other public authorities and clients how we meet our obligations. These records are held and maintained by different functions with regular reporting channels into the Global Data Privacy team responsible for checking compliance with the BCR-C and our data privacy policies and procedures. Our employees understand that they are accountable for maintaining evidence and records where these responsibilities are applicable to their roles.

Compliance with Local Laws

In addition to complying with the BCR-C, each Participating Entity is responsible for taking such additional action as may be desirable or necessary to comply with the data privacy laws and regulations that may apply to the data and/or in the country where it operates. If data privacy laws and regulations in a country require higher level of protection for personal data, they will take precedence over the BCR-C. Upon the request of another Accenture entity or the Accenture Global Data Privacy team, an Accenture entity will supply a copy of such laws and regulations to the requesting party. In addition, to the extent that an Accenture entity from time to time adopts internal procedures designed to promote compliance with such Local Laws and regulations, it will provide the Global Data Privacy team with a copy of such procedures.

In the event a conflict arises in the future due to new Local Laws and the BCR-C, the BCR-C do not override the laws where Accenture operates and to which Accenture is subject. The relevant Accenture Participating Entities will issue instructions to its employees on how to proceed in the interim period until the conflict is resolved.

Privacy by Design - Building privacy into our projects, tools and applications

Accenture considers data privacy as an integral component of the design, development, operation and management of new projects, tools, applications, internal services, and offerings which process personal data. To this end, our Policy 90 and Information Security Policies require our employees to incorporate privacy at the beginning of the design and development stages, adopting technical and organizational measures, such as minimising the processing of personal data, pseudonymising (or anonymizing) personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing When Accenture engages vendors and partner organizations as part of any design, development, and implementation work, we have procedures in place to ensure privacy by design is an integral component.

Privacy by Default

Accenture will use or adopt privacy as the default setting when designing, developing, operating and implementing new tools, applications and other technology used by Accenture and its employees. Accenture will ask its vendors and partner organizations to do the same.

Privacy Reviews, Transfer Impact Assessments and Data Protection Impact Assessments

Privacy reviews and **Data Protection Impact Assessments (DPIA)** are assessment tools used by Accenture group to assess privacy and security risks as part of our risk mitigation procedures. Accenture has a process to initiate privacy reviews to assess our own practices, service offerings, technology to mitigate risks and allow for privacy integration through measures such as privacy by

design or adopting privacy as the default setting. The privacy review may also identify the need for a DPIA.

Not all processing requires a DPIA. We use DPIAs where this is a mandatory requirement for certain types of processing which carry a high risk or have greater implications for rights and freedoms of individuals. The outcome of a DPIA is to identify the necessary measures to minimize risk and comply with the GDPR. Accenture will consult with the Competent Supervisory Authority prior to processing taking place, when required to do so.

Accenture has internal processes in place to manage privacy reviews and DPIAs. All entities are required to act on the outcome of a DPIA or review to help mitigate any privacy risks, including implementing additional measures to mitigate those risks.

Transfer Impact Assessments (TIA)

When an Accenture entity acting as Data Exporter of personal data from the EEA, Switzerland or the UK to another country that was not found to be adequate, such Accenture entity performs Transfer Impact Assessments (TIA) to identify any risk associated with the transfer (including the possibility of access requests by public authorities) and to define supplementary measures to safeguard the data, if necessary.

Accenture will consider when doing a TIA: purposes for which the data are transferred and processed, types of entities involved in the process, economic sector in which the transfer occur, categories and format of personal data, location of processing, and transmission channels.

The completion of the TIA is the responsibility of the Assets Steward in the Accenture team in charge of the specific deal or transfer. The TIA shall include the assessment of the laws and practices of the third country of destination relevant considering the specific circumstances of the transfer and the contractual, technical or organizational safeguards put in place for the transfer. There is no need to repeat the assessment every time there is the same transfer of a specific type of EEA/UK/Swiss personal data to the same Third Country.

Based on the results of the TIA, which will consider the laws and practices relevant to the circumstances, the Data Importer shall inform the Data Exporter if it has reason to believe that it is subject to Local Laws that prevent it from fulfilling its obligations under the BCR-C and agree on supplementary protection measures. The same applies if the Data Exporter has reason to believe that the Data Importer can no longer fulfill its obligations.

In case the Data Exporter or the Data Importer consider that safeguards in addition to those envisaged under the BCR-C should be put in place, the Data Privacy & Information Security Leads supported by the local Geographic Compliance and Corporate team members will be informed and involved in such assessment and in identifying the supplementary measures to be adopted. Such assessment and safeguards shall be made available to the other BCR-C members so that the identified supplementary measures will be applied in case the same

type of transfer is carried out by any other BCR-C member. Where effective supplementary measures could not be put in place the transfers at stake will be suspended or ended, as well as all transfers for which the same assessment and reasoning would lead to a similar result.

Following such suspension, the BCR-C member acting as Data Exporter has to end the transfer(s) if the BCR-C cannot be complied with and compliance with the BCR-C is not restored within one month of suspension. In this case, personal data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the BCR-C member acting as Data Exporter, be returned to it or destroyed in their entirety.

Data Exporters shall monitor, on an ongoing basis, and where appropriate in collaboration with Data Importers, developments in the third countries to which the Data Exporters have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

The TIA and, where needed, the decision on what supplementary measures to implement are documented and centrally stored within Accenture and internally accessible. These are made available to the Competent Supervisory Authority on request.

Audits

Accenture has a privacy compliance audit program. The purpose of the audits is to assess our compliance with our internal procedures and practices, Applicable Data Privacy Laws and the BCR-C.

Different aspects of our auditing program address data privacy compliance. Accenture conducts regular data privacy audits, reviews, and risk assessments, ensuring that all aspects of the BCR-C are effectively monitored over time, including, applications, IT systems and databases. While it may not be necessary to audit every aspect of the BCR-C during each individual audit, we ensure that all BCR-C components are reviewed at appropriate intervals for each BCR member.

There are also regular information security audits and mandatory audits at least every 3 years for any standards or certifications we adhere to, for example ISO 27001/27701.

There is an audit and risk assessment schedule for routine audits and where necessary, we will conduct an audit outside this schedule, under exceptional circumstances. These specific audits (ad hoc audits) may be requested by the Data Privacy Officer or any other competent function in the organisation.

Audits are generally conducted internally by our internal audit function or the Data Privacy Team, and externally by specialized audit organizations. When selecting external auditors, we ensure they are independent and capable of conducting thorough assessments. These auditors are commissioned internally and report their findings to the Chief Compliance Officer and the Sr. Director, Data Privacy. The purpose of these audits is to verify that all processes and practices align with the BCR safeguards for cross-border data transfers,

including adherence to data protection principles and accountability mechanisms.

The person responsible for BCR-C audits must ensure independence. If the Data Privacy Officer (DPO) is involved in these audits, there should be no conflict of interest. The Data Privacy Officer and Global Data Privacy Team can assist BCR members in reviewing and advising in BCR-C compliance, provided no conflicts arise.

All entities agree to be audited by the Supervisory Authorities if required to do so. During the audit, each Accenture entity shall cooperate with the auditor[s] and shall disclose to the auditors any and all information or documents as may be required for the accomplishment of the auditor's objectives,

The results of all the audits relating to the processing of personal data shall be made available to the Senior Director, Global Data Privacy, the Data Privacy Officer and any other relevant Accenture function and market leadership, including relevant boards of directors. Upon request, the results of audits regarding BCR-C will be made available to supervisory authorities.

Audit follow up procedures will include a corrective action plan based on the audit findings and procedures for ensuring the corrective action is implemented.

Liability

Data subjects can then enforce the BCR-C against any relevant Participating Entity for breaches it has caused of the BCR-C. Accenture has accounted for how it manages these enforcement rights within our Accenture Privacy Agreement. Accenture has appointed a specific entity (Accenture Global Holdings Limited) based in the EEA as our Data Privacy Administrator to act on behalf of all Accenture Participating Entities (EEA/non-EEA) for the purposes of the BCR-C. The Data Privacy Administrator is responsible for taking necessary actions to remedy the acts of other Participating Entities outside the EEA and to pay any damages as a result of violations of the BCR-C.

Accenture has addressed liability within our Accenture Privacy Agreement that includes provisions which deal with how Accenture assigns responsibilities, remedies, and liabilities under the BCR-C. The BCR-C member that has accepted liability will have the burden of proof to demonstrate that the BCR-C member outside the EU is not liable for any violation of the rules which has resulted in the data subject claiming damages.

A summary of the Accenture Privacy Agreement can be shared with Data Subjects upon reasoned request, and solely for the purpose of exercising their third-party beneficiary rights.

Employee violations of these BCR-C, Accenture policies or procedures and raising concerns

Violations of the BCR-C may lead to disciplinary action (up to, and including, termination of employment). While Accenture retains discretion as to how to

respond to any violation of the BCR-C, any disciplinary process will be undertaken in accordance with Local Laws and other legal requirements. Employees who have concerns about any issue that they believe (or suspect) may violate any law or violate the Accenture group's COBE, the BCR-C or Accenture group policies, have a right to speak up and we want them to speak up. Employees should refer to our internal policies on Raising Legal and Ethical Concerns and Prohibiting Retaliation for more information.

Annex 2: Categories of individuals, categories of personal data and processing, purposes, recipients, countries

Available as a separate document. It is integrated into the BCR-C document for online publication.

Annex 3: Individuals Rights Requests and Complaint Handling Procedure

Table of Contents

1. Purpose
2. Who handles IRRs and Complaints?
3. Making a request?
4. Submitting a request
   4.1. What is a request?
   4.2. What do individuals need to know?
5. How Accenture manages a request
   5.1. Assigning Case Owners
   5.2. Request management
   5.3. Additional Considerations
6. Escalation options
7. How does Accenture manage complaints?
8. Record Keeping, reports and further action

Owner	Global Data Privacy team	Effective Date of this Version:	2023
Sponsoring Organization:	Legal	Supersedes the Version Dated:	2022
Applies to:	All Accenture BCR-CParticipating Entities and employees	Original Effective Date:	2009

1. Purpose

This document explains Accenture's procedures for handling individuals' rights requests (IRR) under Applicable Data Privacy Laws, for example, subject access and data privacy complaints [referred to jointly as requests]. It does not govern how Accenture handles non-data privacy requests, which are managed separately.

This procedure applies where Accenture is a data controller and to all Accenture entities which are signed up to Accenture's Binding Corporate Rules (BCR-C).

2. Who handles IRRs and Complaints?

Accenture has a Senior Director Global Data Privacy (Director), a Data Privacy Officer (DPO), and a network of Data Privacy & Information Security Leads (DPISL) who will primarily deal with requests. The DPISLs are supported by the Global Data Privacy team providing expertise as and when required.

3. Making a request

For IRRs, individuals or their representatives may only make a request relating to that individual's data and only where Accenture processes his/her information in its capacity as a data controller (for example, in relation to current and former employees, job applicants, client contacts, supplier/vendor contacts and website users whose personal data is processed by Accenture). Anyone can make a complaint about a data privacy matter. These procedures do not apply where Accenture operates as a data processor.

4. Submitting a request

4.1. What is a request?

An individual can submit an IRR where he/she wishes to exercise the following rights given to individuals under Applicable Data Privacy Laws or the BCR-C (to learn more about these rights and what they mean, refer to Section four – Respecting Individuals Rights within the BCR-C Commitments or the Definitions):

- Right of Access;
- Right to Rectification;
- Right to Restrict Processing;
- Right to Erasure;
- Right to Data Portability;
- Right to Object;
- Rights in relation to automated decision making and profiling;
- Rights in relation to making data privacy complaints

or submit a data privacy complaint where the individual considers:

- a breach of the Applicable Data Privacy Laws or regulations has taken place; or

- there is non-compliance with the BCR-C.

An individual can exercise his/her rights regardless of whether he/she makes a complaint to Accenture or a supervisory authority.

4.2. What do individuals need to know?

Request format: Requests should be made in writing and preferably, electronically using either the case management tool or by email to DataPrivacyOfficer@accenture.com, as applicable. Requests can also be sent by post clearly marked for the attention of the Data Privacy Officer, Accenture Limited Dublin, 1 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland. Requests can be made via one of the Participating Entities' offices but should clearly be marked for the attention of the Data Privacy Officer, care of the Legal Department to ensure the request is routed correctly.

Request type: Individuals can submit more than one request at a time and should consider submitting them together along with details of their requested outcome.

Identity verification: Individuals will usually be asked to verify their identity providing suitable identification documentation when this is necessary.

Personal information required by Accenture: Individuals will be asked to provide some of their personal data necessary to deal with their request (unless this has already been provided as part of an initial communication), for example:

a) Contact details

b) Information necessary to facilitate the request, for example:
   - the data to be corrected or deleted
   - information in support of an access request, for example, information to help Accenture locate the relevant data where the requested data relates to Accenture's electronic mail systems

c) their preferred outcome or resolution

Self-service options: In some instances, individuals (both internal and external) will be able to partially manage their requests themselves, for example, setting their marketing preferences through self-service tools, where available.

Appointing a representative: Individuals may choose to appoint a representative to act on their behalf and Accenture may need to seek additional information to verify this appointment before proceeding with the request and/or disclosing any information.

Communications: Upon receipt of a request, Accenture will send an acknowledgement. Accenture may need to communicate with individuals at various intervals to resolve a request. These will generally be made electronically unless Accenture and the individual/their representative have chosen another method of communication.

Closing a request: Accenture will inform individuals when their request has been dealt with and the relevant outcome. Section 5.2 provides an overview of how we respond. A request will be considered closed, provided individuals require no further action.

Escalating a request*:* If an individual requires additional action to be taken or is dissatisfied with the outcome, they can escalate the matter. Additional action may include opening a new request, asking for an additional review or escalating the matter as a complaint. If the matter is escalated as a complaint, Accenture will manage this in line with section 7 of this procedure.

5. How Accenture manages a request

This section explains the Accenture Participating Entities' procedures for managing their respective requests. This procedure is without prejudice to any provisions and requirements of Applicable Local Laws and regulations, including but not limited to labor laws.

5.1. Assigning Case Owners

A DPISL will be assigned as Case Owner according to criteria determined by Accenture. Case Owners will handle requests in compliance with the BCR-C/Applicable Data Privacy Laws using this procedure and the internal processes and guidance which support this procedure.

Certain situations may warrant an exception to the appointment of a particular Case Owner, for example, where there is a dispute or conflict of interest. In these instances, Accenture has procedures in place to appoint an alternative Case Owner.

5.2. Request management

Details relating to requests are generally held in a central case management tool with controlled access. In some instances, details about a request may be logged and held locally where, for example, it is in the overriding interest of the individual or where there are Local Law requirements which require Accenture to hold and process the data locally.

Case Owners generally follow the same process for handling all request types which can be summarized as follows:

Assessing requests: The Case Owner will decide how best to manage the request and which departments or functions need to be involved. If an individual makes multiple requests or the request is complex, the Case Owner may request additional resources and/or expert advice.

Action required: For each request type, Accenture has a set of associated actions for the Case Owner to follow to manage the request and where relevant, apply any exceptions. The Case Owner will also assign relevant actions to individuals from Accenture functions or suppliers who must fully co-operate with the Case Owner in a timely manner.

Documenting decisions: For record keeping purposes, we maintain a record of relevant decisions which are documented within the Case Management Tool.

Timeline: For most requests, Accenture will respond within one month of receipt or according to the specified timeframe (if one month or less but no more than one month) under Applicable Data Privacy Laws. This excludes the time it takes to verify an individual or their representative's details or waiting for further

information from the individual in order to process their request. For some requests, data privacy laws provide circumstances where Accenture has the option to allow an additional two months to respond. Individuals will be made aware of Accenture's delayed response time and the reasons why as soon as Accenture becomes aware of a delay.

Responding to an individual about their request: Where the request has been dealt with, the individual will be informed and supplied with any relevant information/evidence relevant to the request. IRRs are generally resolved as follows:

a) *Subject Access requests:* Accenture will provide the individual with a copy of the information as required under relevant privacy laws. Where the request has been made electronically, we will provide the information securely in a commonly used electronic format unless the individual requests an alternative format with which we can reasonably and securely comply.

b) *Data portability requests:* Accenture will provide the information in a structured, commonly used and machine-readable format and securely transfer the information directly to another data controller at the request of the individual, where this is technically feasible.

c) *Rectification, erasure, restriction:* If the request is assigned a Case Owner and where the request is justified, the Case Owner will instruct the relevant department or function to correct, complete, restrict or erase the data. In some instances, the individual will have self-service options to manage this themselves and it may not be necessary to assign a Case Owner.

d) *Objections:* The Case Owner will ask the departments or functions concerned to record such an objection on the relevant system, stop using the data in question, or where applicable, delete the relevant data and cease using the individual's data for these purposes. Where an individual can manage their own marketing/communications preferences, the Case Owner will highlight this to the individual, however an individual still has the right to ask Accenture to manage these on their behalf.

e) *Automated Decisions:* The Case Owner will report back to the individual on the outcome of their investigation, including an explanation of the decision and where applicable, be given the opportunity to offer their opinion and/or challenge the decision.

Refusing a request: There may be exceptions within applicable privacy/other laws where Accenture has legal grounds to reject or only partially comply with a request. For example:

- the information requested is subject to legal proceedings or is part of an ongoing law enforcement investigation and Accenture is prohibited from disclosing the information, or
- Accenture has received a request to erase an individual's information, but Accenture is obliged to retain the information in compliance with overriding legal requirements such as employment or tax law.

Case Owners will apply any relevant exceptions on a case-by-case basis and maintain a record of such decisions. The Case Owner will inform the individual (unless prohibited to do so) that Accenture is unable to respond to his/her request and specify the reasons for the decision (unless prohibited to do so) explaining where the individual can seek alternative recourse via a supervisory authority or the courts.

Closing a Request: The request will then be closed, and a corresponding record retained pending any further action and in line with Accenture's Retention Policy. In the event the individual contests the outcome or makes a complaint, the Case Owner will follow Accenture's escalation processes as outlined below.

Escalating a Request: The Case Owner will explain to an individual that in the event they are dissatisfied with the outcome, they may consider the escalation options explained in section 6 of this procedure.

5.3. Additional Considerations

a) *Onward notifications:* For requests where Accenture may be required to inform other Accenture and/or third-party entities of the request, the Case Owner will instruct the department or function concerned to communicate the matter to those entities, unless such operation is impossible or involves a disproportionate effort.

b) *Requests sent elsewhere within Accenture – what happens?* Any Accenture function which receives a request should forward it to DataPrivacyOfficer@accenture.com *without undue delay* to enable Accenture to process the request within the legally specified timeframe.

If a request is not referred to the appropriate team at all or with enough time to manage the request within the specified timeframe. As soon as it becomes aware, Accenture will look to take appropriate action to prevent this from happening again.

6. Escalation options

Making a complaint to Accenture: Individuals have the right to come directly to Accenture for resolution of complaints concerning non-compliance with these BCR-C or Accenture's Global Data Privacy Policy. These will be dealt with in accordance with this procedure and our corresponding internal processes and guidance. We encourage and welcome individuals to come to Accenture first to seek resolution of any complaint. Individuals can make a complaint directly to Accenture by following the same process specified in section 4.2I.

Making a complaint to a supervisory authority: Individuals also have the right to register a complaint directly with the relevant supervisory authority. In some complex situations, Accenture may have already consulted with a supervisory authority before reaching its decision. If this is the case, Accenture will make the individual aware of this. This could be the supervisory authority where the individual lives or works or where the alleged data privacy infringement occurred. It is up to the individual to decide which supervisory authority they wish to deal with. A full list of all the EU Member State supervisory authorities is available here.

Making a claim: Individuals can also make a claim against Accenture via a competent court subject to Local Laws. Accenture has the right to object where we have such rights. The competent court is recognised as being in the member state of the European Union where the individual (habitually) resides or where the relevant Accenture controller has an establishment. It is up to the individual to decide which competent court they would look to register a claim with.

7. How does Accenture manage complaints?

General procedure*:* Complaints are generally managed by Accenture in the same way as IRRs and in line with the process referred to in section 5.2.

Specific requirements*:* There are some additional steps Accenture takes in relation to complaints. If a complaint is made against one or more specific individual(s) or, if during the review of a complaint (or as a result of an IRR), it becomes clear that an individual may be responsible for a breach of the BCR-C, our Data Privacy Policy or national laws, Accenture will need to investigate. Any such investigation will be conducted in line with our internal procedures. Where necessary and so as not to prejudice the rights of the individual complainant or the rights of the individual who is the subject of the complaint, the Case Owner will seek further advice and guidance as required from the Global Data Privacy team and other relevant parties including external legal/other professionals.

Individuals who are implicated in a data privacy investigation will be notified with a copy of any relevant procedures. This notification will not be made where it would prejudice the conduct and the outcome of the investigation.

Resolving Complaints*:* Where a specific complaint is justified, the Case Owner shall use reasonable efforts to resolve the situation which led to the complaint. Accenture will take any appropriate action against any individual who has breached the BCR-C, the Data Privacy Policy or Applicable Data Privacy Laws and regulations, in accordance with Local Laws and regulations, including but not limited to employment laws.

8. Record Keeping, reports and further action

General*:* Accenture will maintain details relevant to the request including communications and documentation in accordance with its Retention Policy or in line with any Applicable Local Law requirements. For exceptional circumstances, such as litigation, retention may be longer and will be decided on a case-by-case basis. Accenture maintains these records for its own compliance purposes and in the event the individual escalates their request or complaint to a supervisory authority or engages in legal proceedings against Accenture.

Accenture keeps information including logs of the number and types of requests we receive and how we respond. Some of the information will be communicated internally to help improve our procedures and if required, to provide this information to the supervisory authorities.

Specific reports*:* Upon closing a request, it may be necessary to produce a report where further action is required internally, for example, where we may need to revise our practices and procedures. The criteria for any such report and subsequent outcomes are a decision for the Global Data Privacy Team.

Corrective action*:* Accenture monitors requests carefully. If it becomes apparent that Accenture needs to change the way it processes personal data, Accenture will take reasonable steps and institute a corrective action program to comply with the BCR-C.

For example, if a report states that an offence has been committed or exposes Accenture to increased risk or liability, or if the report recommends a more serious modification of the internal procedures applied for the processing of personal data, there are internal guidelines for escalating the matter to determine how to proceed further and who to involve.

Recipients*:* The Case Owner decides on a case-by-case basis, and after consulting the Global Data Privacy Team where appropriate, on the recipients of a report. The recipients of the report have a right to communicate their observations, especially where Accenture may need to take further action to prevent a similar situation in the future.

Annex 4: Definitions

Available as a separate document. It is integrated into the BCR-C document for online publication.

Annex 5: Accenture Intercompany Agreement – Accenture Privacy Agreement

This is an internal document which is made available to the supervisory authorities but is not published on the Accenture.com website.

Annex 6: Supporting Documentation and Resources

This section lists some of the resources, guidance documents and information available to Accenture employees to help them comply with the BCR-C and understand how Accenture processes their personal data. Data privacy documents and other relevant documents are made available via our internal sites and resources to employees. These documents are not part of the BCR-C and are not available for external publication but would be made available to supervisory authorities where required. They include:

General:

Accenture and Avanade Codes of Business Ethics (COBE): COBE shape the culture and define the character of our company.

Accenture group Data Privacy Statements: The statements (e.g., Accenture Global Data Privacy Statement) explain how and why Accenture processes employees' personal data, who has access to the data and how employees can exercise their rights in relation to their data. The statements provide an overview of Accenture's most common processing activities. Specific processing activities may be subject to a separate and tailored privacy statement.

Data Privacy Tool: The tool is available internally for Accenture employees to submit general data privacy queries or requests for training, Privacy Reviews or review or mobile apps, for example.

Data Privacy Chatbot: The Chatbot is an information resource available for employees to ask routine data privacy questions.

Policies & Standards:

Accenture group policies may vary slightly to accommodate the needs of each Participating Entities, but they all align to the same principles and are driven by Accenture's guidance.

Policy 90 – Data Privacy Policy: the purpose of this policy is to set out the duties of Accenture and our employees when processing personal data about individuals. The BCR-C Commitments are based on this Policy.

Policy 1431 – Data Management: contains governance and direction for all reasonable and appropriate steps necessary to identify, classify and protect all forms of personal, confidential, business and other protected or regulated data that is Accenture Data or Client Data, as defined in that policy.

Data Classification & Protection Standard: this standard defines the different classification levels used by Accenture Participating Entities to comply with Accenture Policy 1431.Data Management and Avanade Policy 5007 Data Classification and Protection Standard

Policy 69 – Confidentiality: outlines responsibilities for protecting confidential Accenture, client and third-party information entrusted to employees.
Policy 1413 – Corporate Records and Information Management: defines Accenture's records retention criteria for specific functions and/or legal, regulatory, and business requirements.
Policy 57 – Acceptable Use of Information, Devices and Technology: includes the requirements for the protection and use of Accenture, client, and other third-party information, devices, and technology. Avanade Policy 1005- "Acceptable Use" is the equivalent to this policy.
Policy 1461 – Social Media: provides guidance to employees on using social media. Avanade policy 0052- "Social Media" is the equivalent to this policy.

Internal Guidelines and Global Templates

Accenture Participating Entities share similar guidelines and standard templates to use when creating contracts or obtaining consent for data processing and in various other circumstances. The templates can be obtained by employees from the Accenture internal Data Privacy site. Not all employees have access to everything. Access is restricted in some instances to legal and compliance teams. The templates may be reviewed by local counsel and localized as necessary to meet legal requirements of specific jurisdictions. These include, but are not limited to:

General Global Notice: for use when consent is not required.

Consent and Notice Template and Guidance: for use when consent is required.

Additional notice: consent implementation guidance for Asset Stewards.

Privacy by Design Guidance: Data Protection by Design Checklist for CIO.

Privacy Statements: Accenture Privacy Statement and Avanade Privacy Statement.

Vendor Templates: Data Privacy Schedules (different schedules have been produced for different scenarios involving vendor processing of Accenture personal data).

Procedure Document: Handling of Government Requests for Personal Data.

Annex 7: Revision History

March 2024 - Revised to include updates of text and Annexes 2 and 4 to accommodate EDPB Referential 1/2022.

March 2023 - Minor revisions to accommodate adoption of BCR-C by Avanade, and the use of Accenture Privacy Agreement as renewed Intercompany Agreement.

March 2022 - Revised to include commitments following the CJEU ruling in the case Data Protection Commissioner vs Facebook Ireland Ltd and Maximillian

Schrems, 16 July 2020, C-311/18 and the final version of the EDPB Recommendations 01/2020.

March 2021 - Refreshed Annex 2 in line with Accenture’s privacy statements and minor revisions following annual update to Irish Data Protection Commission

March 2020 - minor revisions following annual update to Irish Data Protection Commission

March 2019 - Minor revisions following annual update to Irish Data Protection Commission (BCR-C Supervisory Authority) – revisions available upon request.

2018 - Revised and rewritten for GDPR compliance

December 14, 2015 - Updated 'Data Privacy Officers Global List' under the Supporting Documentation section.

August 3, 2015 - Updated contact information.

May 21, 2015 - Added link to Croatia supplement.

September 16, 2014 - Updated policy for CaA Phase 3. Updated 'Data Privacy Officers Global List' under the 'Supporting Documentation' section.

May 19, 2014 - Updated Contact Information.

April 14, 2014 - Reviewed for clarity and consistency.

March 26, 2014 - Site maintenance; no content changes.

March 17, 2014 - Replaced links and references to policy 0078.

January 8, 2014 - Added 'Security Breach Notification Procedures' to the Supporting Documentation section.

August 22, 2013 - Updated link to Social Media Policy under Supporting Documentation Section

December 1, 2012 - Updated terminology to reflect Leadership Careers model.

November 21, 2011 - Corrected a minor typo error.

October 13, 2011 - undo changes to section 2.4 pending further review.

October 10, 2011 - Updated section 2.4, to include wording on data not collected.

March 18, 2011 - Link to the Company’s Social Media Guidelines added under Supporting Documentation.

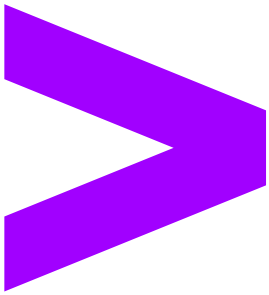
January 27, 2011 - Updated link to Data Privacy Officers Global List in supporting documentation section; no changes to content.

January 25, 2011 – Various changes to substance of the Policy to accommodate comments from regulators in the context of Binding Corporate Rules approval. Also updated supplements and supporting document sections.

November 29, 2010 - Updated list of Data Privacy Officers; no changes to content.

May 25, 2010 - Updated link and reference due to Policy 0057 title change.

March 2, 2010 - Updated list of Data Privacy Officers; no changes to content.



Accenture and its logo are trademarks of Accenture.