ACCENTURE BINDING CORPORATE RULES

("BCR")

accenture

EXECUTIVE SUMMARY

INTRODUCTION

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

Accenture's BCR has been in place since 2009, following an approval process conducted by the European Union data privacy regulators. The BCR was updated in 2018 to reflect new requirements under the EU General Data Protection Regulation.

SCOPE

This document defines obligations Accenture has in regards of data processing in scope of the BCR, 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 apply to all personal data processed by Accenture as a data controller for our own purposes. It does not apply to Accenture as a data processor for services we provide to clients.

The BCR does not override any applicable national data privacy laws and regulations in countries where we operate.

ACCENTURE'S BCR COMMITMENTS

Accenture's data privacy obligations under the BCR 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 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 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 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 BINDING?

Accenture's BCR is made binding on all participating entities using an Intercompany Agreement (ICA). All participating Accenture entities and their employees are bound by the BCR, 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

Annex 1 provides an overview of how Accenture manages its BCR. Day to day responsibility for managing the BCR 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, please direct them to Accenture's Data Privacy Officer:
DataPrivacyOfficer@accenture.com

Table of Contents

Table of Contents

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)

• 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

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 Commitments and associated Annexes:

- Annex 1: How Accenture complies with its BCR,
- 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; which set 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 and how to contact us.

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

- Annex 6: Accenture Supporting Documentation,
- Annex 7: Revision History.

The BCR reflect the standards contained in European data privacy laws and have been approved by most data privacy regulators in Europe. Having BCR means that all our group entities which sign up to them 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 address ethical and legal compliance, accountability, opportunities and risk. All Accenture entities and employees bound by these BCR, 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 here; Annex 4, Definitions .

APPLICABILITY AND SCOPE

APPLICABILITY

Accenture's BCR 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 Commitments:

a) Require all Accenture 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 do not apply to Accenture as a data processor for services we provide to clients. Please note that these BCR do not apply to services we provide to clients. For client-owned 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 national data privacy laws and regulations in countries where we operate.

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 and their locations, click here.

CATEGORIES OF INDIVIDUALS, CATEGORIES OF PERSONAL DATA AND PROCESSING, PURPOSES, RECIPIENTS, COUNTRIES

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. 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 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 BCR 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:
PPROCESSING 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 Commitments, our Data Privacy Policy, (and 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 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 purposes and respective processing

(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

(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 the individuals with any additional information necessary to process the data fairly, transparently and lawfully. This information will include the categories specified above (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 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, and if so, 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 data protection 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 and 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 an individual's data when one of the following applies:

a) If 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.

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, it will inform the individual.

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 defence 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 upon, there must be suitable safeguards such as 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 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 Data Protection Impact Assessment (DPIA) or privacy review, 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 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.

DATA SECURITY BREACHES

Accenture has policies, procedures and protocols in place for managing and responding to data security breaches. 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 Accenture 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 entities and relevant members of the Global Data Privacy Team of the incident and where required, notifying the supervisory authorities without undue delay. In addition, where required notifying 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 data security 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 in accordance with applicable laws.

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 processer (and where relevant, 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 applicable laws;

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

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 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,

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 cross-border transfers take place.

Accenture has put in place procedures for implementing these safeguards to cover our day-to-day processing, for example, via these BCR for internal transfers, or procurement contracts that include the relevant obligations conferred upon processors or 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.

NINE - ACCENTURE'S COMPLIANCE WITH ITS BCR

(a) Accenture has internal arrangements to:

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

(ii) allow individuals to effectively exercise their rights guaranteed under these BCR 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.

(b) All individuals may rely upon these procedures and/or exercise their rights provided for in the BCR 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 commitments (or would have such an effect if the requirements were not imposed on the Accenture entity by law) it will inform the Data Privacy Officer and/or 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, 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

The Accenture BCR are made available via the Accenture.com website to external parties and internally via the Accenture internal portal. Where we are required to publish the BCR in a local language, we will do so. Upon request, we will also e-mail an electronic PDF version of the BCR to an individual.

CONTACT INFORMATION

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

ANNEX 1: HOW ACCENTURE COMPLIES WITH ITS BCR COMMITMENTS

PREAMBLE

The purpose of this Annex is to set out the rules and the procedures to be followed by all Accenture entities and employees to ensure compliance with the BCR Commitments. The BCR 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

To help manage our data privacy program, Accenture has a Global Data Privacy Team led by a Senior Director, Global Data Privacy. We also have a Data Privacy Officer (DPO). Across the regions where we operate, we have a data privacy network which includes Data Privacy & Information Security Leads and Sponsors supported by Geographic Legal Leads, 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 and applicable data privacy laws and regulations at global, regional and country level. The DPO reports into the Senior Director but also has the right to directly escalate issues to other senior leadership within Accenture, including board level, the 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.

MANAGING THE BCR

Day-to-day responsibilities for managing the BCR sits with the Global Data Privacy Team. This includes routine monitoring and reporting. Routine auditing of the BCR 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 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;

b) maintain a full list of the BCR members and ensure this list is up to date;

c) develop audit controls for the BCR;

d) monitor compliance with the BCR;

e) record and track all changes and updates to the BCR and the rationale for the updates and provide this information, where necessary, to Accenture BCR entities or the Supervisory Authorities, as required or as part of our annual update;

f) communicate with the competent Supervisory Authority and BCR entities, if a proposed change to the BCR either affects the level of protection offered by the BCR or significantly affects the BCR, in particular, its binding nature; and

g) communicate any other relevant matters to the competent Supervisory Authority or other supervisory authorities where necessary.

COOPERATING WITH THE SUPERVISORY AUTHORITIES

GENERAL COOPERATION PROCEDURES

All Accenture entities have a duty to cooperate with the Supervisory Authorities (SA) for information or inspection. Each Accenture entity will comply with their advice on any issues relating to the BCR, (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 SA) , 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 until they have signed the Accenture intercompany agreement and are effectively bound by the BCR. However, we may use other transfer mechanisms to facilitate transfers until they join the BCR. Changes to the BCR entity list will be reported to all Accenture entities signed up to the BCR and to the relevant supervisory authorities via the competent SA.

REPORTING MATTERS TO THE COMPETENT SUPERVISORY AUTHORITY

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

Conflicts between local laws and the BCR: Accenture has a duty to inform the supervisory authorities of any conflict between local law requirements and the BCR 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.

Disclosure and transfer requests: All Accenture entities agree that transfers of personal data to any public authority or body cannot be massive, disproportionate and indiscriminate.

All Accenture entities must report any such disclosure requests to the Accenture Data Privacy Officer and/or Global Data Privacy Team. The Data Privacy Officer/Team will then inform the competent SA about the request, the identity of the requesting party and the legal basis for the request [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 SA with as much information as possible to be able to evidence their efforts to do so. All Accenture entities must keep a record on the disclosure requests it receives. 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. The Accenture entities must provide the competent SAs with an annual update of these records.

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. All Accenture employees who regularly process personal data will be given appropriate and timely data privacy training. 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 DPO and/or members of the Global Data Privacy Team responsible for checking compliance with the BCR 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, each Accenture entity is responsible for taking such additional action as may be desirable or necessary to comply with the data privacy laws and regulations in the country where it operates.

Upon the request of another Accenture entity or any of 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 DPO and 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, the BCR do not override the laws where Accenture operates and to which Accenture is subject. The relevant Accenture 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, there is internal guidance and processes on how to incorporate privacy as an essential part at the beginning of the design and development stages. 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, apps and other technology used by Accenture and its employees. Accenture will ask its vendors and partner organizations to do the same.

DATA PROTECTION IMPACT ASSESSMENTS AND PRIVACY REVIEWS

Data Protection Impact Assessments (DPIAs) and privacy reviews are assessment tools used by Accenture to assess privacy and security risks as part of our risk mitigation procedures. We useDPIAs 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.

Not all processing requires a DPIA. In these instances, 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 outcome of a privacy review may also be the need for a DPIA.

Accenture has internal processes in place to manage DPIAs and privacy reviews. 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.

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.

Different aspects of our auditing program address data privacy compliance. Audits will generally be carried out at regular intervals but also by exception, where there is a particular need to conduct an audit outside of the regular schedule. Audits are conducted internally by our Compliance Monitoring Team, our Internal Audit function, the Data Privacy Compliance team or an external organization, specializing in audits. Accenture conducts regular reviews and regular risk assessments for data privacy. There are also regular information security audits. Accenture has developed a series of audit controls against which to monitor our data privacy compliance. These controls cover compliance with the commitments we make in the BCR, our data privacy policies, procedures and processes and compliance with data privacy laws.

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, subject to compliance with local laws and regulations.

The results of all the audits relating to the processing of personal data shall be made available to the DPO, Senior Director, Global Data Privacy, and any relevant Accenture function and geographic leadership. Upon request, the results 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

Accenture has addressed liability within its Intercompany Agreement (ICA). The ICA includes provisions which deal with how Accenture assigns responsibilities, remedies and liabilities under the BCR.

EMPLOYEE VIOLATIONS OF THESE BCR, ACCENTURE POLICIES OR PROCEDURES AND RAISING CONCERNS

Violations of the BCR 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, any disciplinary process will be undertaken in accordance with all applicable local laws and other legal requirements. Employees who have concerns about any issue that they believe (or suspect) may violate any law or violate Accenture's Code of Business Ethics, the BCR or Accenture policies, have a right to speak up and we want them to speak up. Employees should refer to our internal policy 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

This table sets out the types of individuals we **may** process personal data about, the categories of personal data we may process about them, and the purposes for which we process personal information. This table is intended to be a generic summary. It does **NOT** mean we process this data about all these types of individuals.

TYPE	EXPLANATION
Categories of individuals	1. Accenture employees (past and present) - includes permanent and contracting staff [temporary or casual workers, freelancers, contractors, trainees]. 2. Non-employee workers including volunteers, assignees, advisors, consultants, agents and other professional experts, secondees, apprentices, interns, alumni, other third parties. 3. Individuals identified by the aforementioned data subjects as dependents and beneficiaries, including insured spouses and partners, children, guardians and parents, family members and contact persons for emergencies. 4. Job applicants, candidates and pre-hires. 5. Client contacts, current and past contacts and prospects - including employees, officers, agents, consultants and other professional experts. 6. Vendor, supplier contacts. 7. Members of the press and other organizations (including charities, educational institutions, regulators, business intermediaries, etc.). 8. Website users and complainants, correspondents and enquirers. 9. Individuals attending our events. 10. Shareholders. 11. Alumni. 12. Children and adolescents via our Corporate Citizenship, intern and outreach programs. 13. Other third parties.
Categories of personal data and processing	**Personal details [employment context]** - Name, all types of contact details (such as e-mail, phone numbers, physical home and place of work address), gender, date of birth, place of birth, national identification number, social security number, internal company employee or id numbers, marital/civil partnership status, domestic partners, dependents, disability status, emergency contact information, ethnic origin, minority flag, photograph, and images/footage captured on CCTV or other video systems, smart building controls and metric systems used for data analytics, driver license number, car details and other necessary data for use of company cars (including clearing, damage events, insurances), government-issued ID number; military status and rank; emergency contact details; usage/account details of cards for restaurants and vending machines; information obtained through the use of surveys; investigations, complaints and grievances data including as part of the business ethics line; mergers and acquisitions data. **Personal details [clients & prospects]** - Name, all types of contact details (such as salutation, job title, e-mail, phone numbers, physical home and place of work address), contact preferences, preferred language for communications, marketing preferences, data relating to goods and services provided or obtained, relationship with Accenture [prospect, client, alumni now client]; data related to events [invitations, attendance, relevant costs]. **Personal details [vendors, service providers, suppliers, payees and intermediaries, legal services data]** – Name, all types of contact details (such as salutation, job title, e-mail, phone numbers,

physical home and place of work address); preferred language for communications; data related to invitations for business trips or other business events (e.g., itinerary, costs); entity tax identification number and commercial registry registration number; entity nationality; entity bank details and payment related information, bill to and ship addresses, billing currency; VAT (or equivalent) number; customer/vendor/supplier number or other unique identifier; country registration number, where applicable; information derived from the deployment and use of information systems and tools including from third parties; records related to the provision and management of products orders or returns, provision of services, accounts and internal administration and accounting; curriculum vitae; time and expense records concerning the provision of services; operational data; details of relationship with Accenture.

Other individuals [alumni, corporate citizenship/outreach, website visitors] - Name, all types of contact details (such as salutation, job title, e-mail, phone numbers, physical home and place of work address), contact preferences, preferred language for communications, marketing preferences, data relating to interaction or relationship with Accenture - enquiry, complaint, site visit, application for award, grant, educational initiative, competition.

Documentation required under immigration laws - Citizenship, passport data, details of residency or work permit.

Compensation and payroll - Remuneration details (including historic pay, base pay and bonus or incentive pay, salary banding, frequency of payments), pay deductions, tax codes, insurance codes and statutory and voluntary contributions, benefits, loans, overtime and shift work, compensation type, pay frequency, salary reviews and performance appraisals, banking details including credit card details [both company and personal where the employee has used this], working time records (including vacation and other absence records, leave status, hours worked and department standard hours), pay data and termination date, compensation details, reductions/reimbursements, employee/capital-forming investments, expense descriptions, amounts claimed, cost type, approval and pre-approvals, data required to support expenses claims including bills, receipts, documents.

Leaves of absence - Vacation, statutory leaves and voluntary leaves (including maternity and paternity leaves, sabbaticals), justification for paid absences (including education, family events, social activities, children and other dependents' care). Data relating to administration or leave (including start date, end date, temporary suspension), illness including accidents at work and occupational health (in accordance with local law). Dates (beginning, end and duration).

Pension records - Monthly pension, yearly pension, capital sums, deferred compensation sums, type of pension plan; other data related to pension fund (including enlistment and discharges, contribution data and insurance period in the statutory Social Security).

Position - Description of current position, job title, corporate status, career level, management category, job code, job function(s), legal employer entity, location, Accenture contact(s), employee identification number, terms of employment or contract, work history, hire/re-hire and termination date(s) and reason, length of service, executive management responsibility, trade union membership, retirement eligibility, promotions and disciplinary records, date of transfers, and reporting manager(s) information.

Work location & relocation - Working address, place of work (including work place office, home office, shared desk, external work), workplace indicator, work location code, branch office, sales office, building, room, locker, relocation information (including international assignment flag, assignment data and dates, current assignment, future assignment, country, hypotax, tax reconciliation, foreign tax); employment permits (including date); visa country, visa expiration date, mobility preferences, termination date and reason code; assignment responsibility, assignment job title, tasks; employee's willingness to travel or relocate.

Talent management information - Details contained in letters of application and resume/CV (previous employment background, education history, professional qualifications, any technical specialisations or qualifications, trade licenses, language and other relevant skills, certification, certification expiration dates), legal prerequisites for employment, information necessary to

complete a background check, details on performance decisions and outcomes, e-learning/training programs, internal and external certifications and membership of professional associations, performance and development reviews (including information you provide when asking for/providing feedback, creating priorities, updating your input in relevant tools, comments from/re. counselors/counselees), willingness to relocate, driver's license information, and information used to populate employee biographies.

Management records - Details of any shares of common stock or directorships, stock purchase plans, stock purchase eligibility and contribution, stock options information.

Website, tools, systems, apps - Information required to access Accenture systems, tools and applications such as System ID, LAN ID, e-mail account, instant messaging account, mainframe ID, previous employee ID, previous manager employee ID, system passwords, access logs, access rights, security level, activity logs, employee status reason, branch state, country code, previous company details, previous branch details, and previous department details, and electronic content produced using Accenture systems, information derived from the deployment and use of information systems and tools including from third parties; tracking data including data from cookies and other technology, visitor logs, IP addresses, individual posts into chat rooms, blogs, circles, comments, systems' recordings such as web meetings, calls and webinars.

Sensitive data - Certain types of sensitive information when permitted by local law, such as health/medical information, trade union membership information, religion, and race or ethnicity, criminal records, proceedings, outcomes and sentencing. Accenture collects this information for specific purposes, such as health/medical information in order to accommodate a disability or illness and to provide benefits; religion or church affiliation in countries such as Germany where required for statutory tax deductions; and diversity-related personal data (such as race or ethnicity) in order to comply with legal obligations and internal policies relating to diversity and anti-discrimination. Accenture will only use such sensitive information for the purposes provided by law.

Advertising. marketing and public relations - Promoting and providing products and services to actual and potential customers; advertising, marketing and PR related activities; communications; compliance; business operations; research, complaints and enquiries handling; management of business relationships and other activities; other services.

Accounts and records data, data relating to vendors, service providers, suppliers, payees and intermediaries, legal services data - Order management, including billing, credit analysis, shipping, account maintenance, and internal administration and accounting for all commercial relationships; managing and analyzing sales and demand; communications; business operations; customer relationship management (e.g., CRM); conducting internal audits and other internal control activities relating to contract; management with customers, suppliers, vendors, subcontractors and business partners; compliance; due diligence for anticorruption and anti-bribery purposes; reporting activities to fulfil finance and accounts requirements; risk management and corporate audits and assessments (e.g., Background Investigations Tool and Gift & Entertainment Hub) Internal investigations (e.g., Business Ethics Helpline); internal investigations; legal filing and reporting; purchase order and payment; computer system security, including ensuring adequate level of protection of the personal data stored therein; other services on an ad-hoc basis.

Data relating to mergers, ventures and acquisitions - Management and employment information, compensation and payroll data, business operations, customer relationship management, compliance; due diligence, reporting activities to fulfil finance and accounts requirements; risk management and corporate audits and assessments; legal filing and reporting; computer system security, including ensuring adequate level of protection of the personal data stored therein.

Purposes for which Accenture uses personal information	Scheduling Talent Acquisition / Recruitment Management and administration of employees Employee engagement, performance management and professional development

	Financial planning, payroll, fund management and accounting Share plan management and operations Business and market development – Advertising, marketing and public relations Building and managing external relationships Maintaining relationships with former employees and Alumni relations Planning and delivery of business integration capabilities Research and development Compliance, audit and insurance purposes, including supplier and customer due diligence Internal and external investigations including liaison with law enforcement/other government agencies where required to do so by law Litigation management Client, supplier and business intermediary/partner management Technology infrastructure, security and support (including business continuity), facilities and data management, internal business support services Travel management Knowledge management Corporate Citizenship and outreach programs Reporting to data privacy supervisory authorities - routine reporting and breach notification Liaising with regulators/government departments for routine reporting requirements under law – tax, social security, benefits, national ID programs Mergers & Acquisitions - this includes due diligence and information relevant to potential ventures, joint ventures, mergers and acquisitions Other purposes not incompatible with the ones listed above or other purposes required and/or permitted by law or regulation
Recipients	**Accenture entities** - Accenture entities which are signed up to the BCR or other Accenture entities/affiliates outside the BCR [using a different transfer mechanism]. **Professional advisors** - Accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors. **Service providers** - Companies that provide products and services to Accenture such as payroll, pension scheme, benefits providers, human resources services, performance, training, expense management, IT systems suppliers and support, third parties assisting with equity compensation programs, credit card companies, medical or health practitioners, trade bodies and associations, and other service providers. **Public and governmental authorities** - Entities that regulate or have jurisdiction over Accenture such as regulatory authorities, law enforcement, public bodies, and judicial bodies. **Corporate / commercial transaction** - A third party in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of Accenture business, assets or stock (including in connection with any bankruptcy or similar proceedings). A third party in connection with any proposed or actual client project.
Countries to which transfers may be made	Many of our global systems are operated from the US, we also have significant operations in India, Philippines and China. However, as a global group we transfer to many countries worldwide, inside and outside the EEA. We publish a list of group companies that have signed the BCR intercompany agreements which is available here.

ANNEX 3: INDIVIDUALS RIGHTS REQUESTS AND COMPLAINT HANDLING PROCEDURE

Table of Contents

OWNER	Global Data Privacy Team	**EFFECTIVE DATE OF THIS VERSION**	2019
SPONSORING ORGANIZATION	Legal	**SUPERSEDES THE VERSION DATED**	2009
APPLIES TO	All Accenture BCR 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).

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 (to learn more about these rights and what they mean, refer to Section four – Respecting Individuals Rights within the BCR 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 BCRs.

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 the case management tool (current Accenture employees only) or by email to DataPrivacyOfficer@accenture.com. 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 local Accenture 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 the 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 procedure for managing requests. This procedure is without prejudice to any provisions and requirements of applicable national 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 BCRs/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 instance, 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 be 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 their complaints which 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 3.2.

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, 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 BCRs our Data Privacy Policy or applicable data privacy laws and regulations, in accordance with any applicable national 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 is 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.

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

ACCENTURE SECURITY OPERATIONS CENTER (ASOC)

ASOC is where Accenture employees report any information security incidents or breaches, and any physical or personal security emergencies. It can be reached 24 hours a day, 7 days a week, 365 days a year. It is for internal reporting purposes only.

ANONYMOUS, PSEUDONYMISED OR AGGREGATED DATA

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

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

Pseudonymisation or key coding strips away the identifiable information from specific data replacing it with a non-identifiable pseudonym. An individual can no longer be identified from the pseudonymised data alone without linking that data to additional information. The additional information necessary to return the data to an identifiable state would be held separately and securely elsewhere, to prevent re-identification.

Aggregated data is data grouped and summarized from multiple sources for purposes such as data analytics or statistical analysis. In the context of personal data, although the aggregated data is based on identifiable information, once it has been aggregated, the personal identifiers have been removed.

ASSET STEWARDS

Asset stewards, sometimes referred to as asset owners are responsible for the day to day activities necessary to protect information. Their duties include collaborating with data owners who sit within the business to uphold data protection controls.

BINDING CORPORATE RULES

BCRs (Binding Corporate Rules) are an EU mechanism to allow international transfers of personal data across Accenture's worldwide organization. They are legally binding and have been approved by EU data privacy regulators. Accenture entities signed up to the BCRs comply with the same internal rules for processing personal data. Individuals' rights stay the same irrespective of which Accenture location they are processed. BCRs apply to Accenture internal data personal data where Accenture is a data controller and NOT client personal data.

CLIENT DATA PROTECTION (CDP) PROGRAM

Accenture processes personal data on behalf of its clients and has established a Client Data Protection program to establish and assess controls and standards to help reduce business and financial risk to Accenture, our clients, and their clients, customers or employees. The program provides engagement teams with a standardized approach to implement comprehensive and consistent controls to protect client data. To learn more about Accenture's Client Data Protection program which provides engagement teams with a standardized approach to implement comprehensive and consistent controls to protect client data.

COMPETENT SUPERVISORY AUTHORITY

The need for an organization to establish a Lead Supervisory Authority is triggered when there is data processing. For the purposes of a BCR, an organization liaises with one supervisory authority, referred to as the Competent Supervisory Authority as it goes through the approval process. Once approved, an organization such as Accenture will liaise with that supervisory authority on a regular basis for all routine reporting requirements under the BCR.

CODE OF BUSINESS ETHICS (COBE)

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

CROSS BORDER TRANSFERS (DATA TRANSFERS)

Some data privacy laws have specific restrictions on transferring personal data outside a country or region's borders. The transfer can only take place providing there are certain safeguards in place or the transfer meets the criteria set within the specific privacy law.

This includes internal transfers of personal data Accenture makes across its global organisation and to third party suppliers and vendors located outside the EU/EEA. European privacy laws, for instance, require that when such a transfer takes place, additional safeguards, for example, model clauses or BCRs are put in place to protect the data.

DATA CONTROLLER

A data controller is specific to European data privacy laws but is also used in several other, but not all, data privacy laws. The data controller is the decision maker and determines the purposes and means for processing personal data. Accenture is considered the data controller, for example, in relation to employees' data used for employment purposes. When providing services to a client, Accenture is in most cases considered the data processor, the client is the data controller and provides instructions for processing personal data on its behalf. It is possible to have joint data controllers determining the purposes and means of the processing.

DATA PRIVACY GUIDANCE

Accenture has a dedicated data privacy site which hosts a number of data privacy guidance documents accessible to our employees to help them comply with Accenture's BCR, its wider data privacy program and data privacy laws.

DATA PRIVACY & INFORMATION SECURITY LEADS

DP&IS Leads are responsible for managing data privacy matters within their Geographic Unit (GU). They also carry out tasks delegated by Accenture's Data Protection Officer and act as the point of contact for the relevant data privacy regulators. The Data Privacy & Information Security leads are the first point of contact for local data privacy questions from employees.

DATA PRIVACY NETWORK

The data privacy network which includes the Data Privacy & Information Security leads and Sponsors; manage local data privacy compliance activities; and provide guidance for data protection impact assessments, data privacy regulatory notifications, requests and audits, and local data privacy reporting. They are led by the Data Privacy Officer.

DATA PRIVACY OFFICER (DPO)

Accenture has a Data Privacy Officer responsible for reviewing and monitoring Accenture's data privacy compliance supported by the data privacy network.

DATA PRIVACY POLICY (ALSO KNOWN AS POLICY 90)

The purpose of this policy is to set out the duties of Accenture and its employees when processing personal data about individuals. The BCRs commitments are based on this Policy.

DATA PROCESSOR

A data processor is a term specific to European data privacy laws and can be used in other data privacy laws. It is an organization contracted by a data controller that processes data on behalf of that controller. These type of arrangements can also be referred to as third party processing operations and data processors are often referred to as suppliers, vendors or third parties. Accenture uses data processors in a variety of ways, for example, outsourcing travel arrangements, recruitment and some IS services.

As part of our client delivery services, Accenture is in most cases considered the data processor, the client is the data controller and provides instructions for processing personal data on its behalf.

DATA PROTECTION IMPACT ASSESSMENT (DPIA) AND OTHER PRIVACY RISK ASSESSMENT TOOLS (PRIVACY REVIEWS)

Data protection impact assessments, privacy reviews and a CDP risk assessment are all assessment tools used by

Accenture to assess privacy and security risks as part of our risk mitigation procedures.

DPIA: A Data protection impact assessment (DPIA) is the privacy equivalent of a risk assessment and is a mandatory requirement under GDPR for certain types of processing. Any processing which carries a high risk or has greater implications for individuals will require a DPIA to help an organisation mitigate those risks and demonstrate accountability. Examples include processing sensitive personal data, systematic monitoring or profiling. Please note that not all processing requires a DPIA. Generally, the outcome of a DPIA is to identify the necessary measures to minimize risk and comply with the GDPR. Please contact the Global Data Privacy team for more information.

Privacy Review: a privacy review is not a mandatory requirement under GDPR but is a tool for Accenture 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 outcome of a privacy review may also be the need for a DPIA. Please note that privacy reviews will sometimes be referred to as privacy impact assessments. In order to maintain a distinction between a mandatory DPIA and a PIA, Accenture refers to them as privacy reviews. Please contact the Global Data Privacy team for more information.

DATA PRIVACY SITE

There is a dedicated site available to Accenture employees for data privacy resources and relevant information, news and updates.

DATA SECURITY BREACH

Data security breaches can be defined in a number of different laws not just data privacy laws and the requirements can relate to a number of categories of data, including personal data. Within European privacy laws, a "personal data breach" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

EMPLOYEE

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

EUROPEAN ECONOMIC AREA

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

EUROPEAN DATA PRIVACY LAWS

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

EUROPEAN UNION

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

GEOGRAPHIC LEGAL LEADS

The Geographic Legal Leads provide local legal advice and data privacy support as and when required.

GEOGRAPHIC UNIT (GU) DATA PRIVACY & INFORMATION SECURITY LEADS

Geographic Unit Data Privacy & Information Security Leads are the first point of contact for data privacy guidance and questions in each GU.

GLOBAL DATA PRIVACY TEAM

The Senior Director, Global Data Privacy, supported by the Global Data Privacy team, is responsible for setting strategy and the direction of Accenture's global data privacy program and providing guidance on how to achieve compliance with our data privacy ethical and legal obligations. This includes interpreting requirements, setting controls and defining responsibilities.

GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR is the "General Data Protection Regulation", (Regulation (EU) 2016/679) and is effective beginning May 25th, 2018. The new regulation is designed to unify data privacy laws across Europe and to protect and strengthen data privacy within the European Union (EU). GDPR also strives to reshape the way Accenture and other organizations approach data privacy, widening the scope of protection, increasing individual rights, and creating global obligations. EU Regulations are directly applicable which means a Member State has little room, beyond the derogations to interpret the requirements as they do with Directives. In theory, Regulations lead to better harmonization across the Member States.

FINES, PENALTIES & CRIMINAL SANCTIONS

Most data privacy laws impose some form of penalties, fines and criminal sanctions. The severity of these vary from country to country and generally depend on the nature of the non-compliance and the adverse consequences for individuals.

For example, in the US, there are data security breach requirements at state and federal level which impose significant financial penalties for data security breaches and failure to notify breaches. In Canada, there are significant penalties for breaching Canada's Anti-SPAM Law (CASL). Fines can run into hundreds of thousands of dollars (US $) for these types of non-compliances. The GDPR currently has the most significant consequences for non-compliance. These include:

Financial penalties: fines up to 4% of an organization's worldwide annual turnover or 20 million euros, whichever is greater

Processing restrictions: an organization could be ordered to stop processing permanently/temporarily

Compensation: individuals can sue for both material and non-material damage (distress). They can sue data controllers and data processors

Regulatory supervision: data privacy regulators have audit and inspection powers, can issue warnings and enforce individuals' rights

INDIVIDUAL RIGHTS

Some data privacy laws such as the GDPR give individuals specific rights in relation to their data. As a data controller, Accenture must have processes in place to help individuals exercise these rights. While the rights differ according to countries, we have adopted the broadest definition of these rights and they are incorporated within our BCRs. That means someone who works for Accenture in a country with no privacy laws would have the same rights under our BCRs as someone who works in a country with privacy laws. The GDPR includes the most comprehensive set of individuals' rights, which are as follows:

Right to be informed: essentially this is about being transparent with individuals so that they are fully informed about how their personal data will be processed. Information is usually provided to individuals through a data privacy notice which must be written in plain language i.e. easy to understand and easily accessible.

Right of access: many data privacy laws specify a Right of Access which provides individuals with the right to know if and how their personal information is being used by an organisation, and also the right to a copy of the data. Under GDPR, when an individual makes a request, it is referred to as a subject access request (SAR). We must provide them with the data within a legally specified timeframe.

Right to Rectification: an individual has the right to request that an organization rectify inaccurate personal data about them or to have personal data which is incomplete, amended. As with other individuals' rights, the organisation must comply with a request within a specified timeframe.

Right to erasure (Right to be forgotten): the right to erasure is also known as the 'right to be forgotten' and is when an individual can request that their personal data be deleted or removed by a controller for reasons which include:
• the purpose for the processing no longer exists,
• the individual withdraws their consent to the processing,
• it was being processed unlawfully i.e. no basis for the processing, or
• the processing relates to online services aimed at a child.

The individual can request full or partial deletion/removal of the data in question. Accenture has a limited timeframe to respond to such a request and an obligation to inform other recipients of the data about the request to ensure they also comply with the request.

Right to restrict processing: individuals have the right to request a restriction be placed on the processing of their data. Essentially this means that an individual can stop us from using their data under certain circumstances.

Right of data portability: an individual can request a copy of personal data they have provided to a data controller where the processing is either based on their consent or for the performance of a contract. The individual can request that you transfer the information directly to them or another controller. The right relates to automated data which the controller is obliged to provide in a structured, commonly used and machine readable format (however, there is no obligation to ensure system compatibility with another controller) and must be provided free of charge. A data controller must respond to such a request within one month of receipt.

Right to object and automated decision-making: In certain circumstances, an individual can request that a data controller stop processing their personal data. This is known as the right to object. For example, an individual can object to processing of their personal data where this is based on legitimate interests or in the public interest or for direct marketing (including using their information for profiling purposes).

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 GDPR, an individual has the right NOT to be subject to automated decisions which produce legal effects or significantly affect them, to protect them against potentially damaging decisions, made without human intervention. An individual has the right to ask for an explanation 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,
• is for the purposes of a contract or
• authorized by law.

Where consent or contracts are relied upon, there must be suitable safeguards such as 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.

INTERCOMPANY AGREEMENTS

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

LAWFUL PROCESSING

Data Privacy Laws will generally specify a set of requirements for processing personal data lawfully. Providing one of these requirements is met, the processing will be considered lawful. To process sensitive personal data, you will generally need to meet additional requirements in order for the processing to be considered lawful.

For example, the GDPR specifies the following conditions for processing to be considered lawful, a data controller only needs to meet one of these conditions which include, but are not limited to processing, which:
• takes place with the consent of an individual or
• is necessary for the performance of a contract,
• is required to satisfy a legal obligation which the controller must comply with
• is necessary for the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject

LEGITIMATE INTERESTS

European data privacy laws include specific criteria for lawful processing of personal data. The legitimate interests of a data controller are one basis. Defining legitimate interests can be complex and it is worth noting that the legitimate interests of a controller cannot override the rights and freedoms of individuals.

NOTICE, CONSENT AND CHOICE

When we collect personal data, individuals need to know how that data will be used and what their individual rights are, including access and correction. In most instances, we do this by providing a privacy notice (e.g. accenture.com,

surveys, mobile apps). For some of our internal tools, information about how we collect employee information are found at Protecting Accenture.

Many privacy laws, stipulate consent as one of the legal bases for processing personal data lawfully. For example, under GDPR, for consent to be considered valid, it must be a freely given, specific, informed and an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Choice is whereby you put the decision in the hands of the individual in relation to their data. For example, they have the choice to accept or opt-in to direct marketing or settings within an app or tool are set by default to the highest privacy setting possible and it is then their choice to change their settings and set their preferences.

PRIVACY BY DESIGN

Privacy by design means integrating privacy as a design component from the start when developing, designing, selecting and using applications, services and products which process personal data. Privacy should not be an afterthought or last minute addition. It is a legal requirement under European data privacy laws and in other countries with data privacy laws, is considered good practice.

PRIVACY BY DEFAULT

Privacy by default means implementing appropriate technical and organizational measures for ensuring that privacy becomes the default option for processing personal data. For example, only collecting the minimum amount of personal data necessary for a specific purpose and having privacy as the default settings within an app/tool so an individual does not have to amend their settings to safeguard their privacy. It is a legal requirement under European data privacy laws.

PERSONAL DATA

PII (personally identifiable information) or personal data is information which makes an individual directly or indirectly identifiable. Different laws have different definitions but typical examples include employee names or email addresses, vendor and client contact details and recruitment and alumni data. Accenture uses the broadest possible definition of personal data.

PROCESSING

Processing (specific to European privacy laws) is an all encompassing term to describe anything which involves personal data. The definition is so extensive, it is very difficult to claim an operation or set of operations performed on personal data do not constitute processing under GDPR. For example, viewing, access, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, use, disclosure, transmission, dissemination, alignment or combination, restriction, erasure or destruction.

REGULATORS

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

SENSITIVE PERSONAL DATA

The definition of sensitive personal data varies by country but can include:

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

SUPERVISORY AUTHORITY

The supervisory authority is the term used to describe a data privacy regulator with delegated responsibility for supervising data privacy in a particular country. European Member States generally refer to their data privacy regulators as supervisory authorities.

ANNEX 5: ACCENTURE INTERCOMPANY 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 and understand how Accenture processes their personal data. Data privacy documents and other relevant documents are made available via our internal site and resources to employees. These documents are not part of the BCR and are not available for external publication but would be made available to supervisory authorities where required. They include:

GENERAL:

Accenture Code of Business Ethics (COBE): Accenture's Code of Business Ethics shapes the culture and defines the character of our company.

Accenture Global Data Privacy Statement: The statement explains 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 Statement provides 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, Data Privacy Impact Assessment 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:

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 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 to comply with Policy 1431.

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.

Policy 1461 – Social Media: provides guidance to employees on using social media.

INTERNAL GUIDELINES AND GLOBAL TEMPLATES

Accenture also has 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.

Notice: privacy statement for the Accenture.com website.

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

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

ANNEX 7: REVISION HISTORY

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

2018 – Revised and rewritten for GDPR compliance.