Accenture Processor Binding Corporate Rules (“Processor BCR”)

October 2023

accenture

Table of Contents

Introduction

Purpose

The purpose of this document is to:

- explain Accenture's data privacy obligations as a Data Processor and/or Sub processor under these EU Processor Binding Corporate Rules (Processor BCR).
- explain the Processor BCR scope and application.
- define Employees' data privacy responsibilities and accountability within this scope.
- explain how Accenture handles applicable complaints/queries and Individual Rights under the Processor BCR.
- provide information on how to contact Accenture directly.

Legal background

Applicable 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 processing of Personal Data, we are a decision maker, generally referred to as a "Data Controller". Where we act as a service provider to process Personal Data on behalf of others – typically our Clients – we are a "Data Processor". (Please note that these terms are not necessarily prevalent across all Applicable Data Privacy Laws or may be defined differently.)

There are strict EU Data Privacy Laws requirements on transferring Personal Data outside the European Economic Area (EEA) to another country. These requirements apply to all Cross Border Transfers of Personal Data outside the EEA, including internal transfers of data within a group of companies. Unless certain exemptions apply, such Cross Border Transfers are generally only allowed if a substantially equivalent level of protection has been put in place using mechanisms recognized by EU Data Privacy Laws. Binding Corporate Rules (once approved by EEA regulators) are an example of such mechanisms.

Accenture's Controller and Processor BCR

In order to ensure compliance with Applicable Data Privacy Laws both when acting as Data Processor and as Data Controller, Accenture has in place Processor Binding Corporate Rules (Processor BCR) and Controller Binding Corporate Rules (Controller BCR) which govern how Accenture processes Personal Data as a Data Processor and as a Data Controller respectively.

These Processor BCR govern how Accenture entities process Personal Data on behalf of Clients which are Data Controllers and are binding for all the entities within the Accenture group that sign the Intracompany Agreement ("ICA") to be bound by these Processor BCR, including Accenture Global Holding Limited. These Processor BCR are therefore legally binding on all Participating Entities that must integrate them within their operational practices.

Both sets of BCR reflect the standards contained in EU Data Privacy Laws and have been approved by EEA data privacy Regulators. Participating Entities and their Employees, irrespective of geographic location and in relation to all their processing activities, regardless of whether they act as data exporters or importers, abide by the same internal set of rules – establishing appropriate and uniform data privacy safeguards across our organization. It also means that Individual Rights stay the same no matter where individuals' Personal Data is processed by Accenture Participating Entities. Accenture has a global data privacy program to manage these obligations and address ethical issues and legal compliance, accountability, opportunities and risk.

Accenture's Controller BCR can be found here. You can find the explanation of the data privacy terms used in these Processor BCR here.

Accenture's Processor BCR are comprised of a set of Processor BCR obligations and associated *Annexes:*

- Annex 1: *How Accenture complies with our Processor BCR,*
- Annex 2: *Categories of individuals, categories of Client Personal Data, processing, purposes recipients, countries,*
- Annex 3: *Definitions, and*
- Annex 4*: Intercompany Agreement-Accenture Privacy Agreement,*

which set out Accenture Participating Entities' data privacy obligations, the safeguards we have established to meet those obligations, how we manage Individual Rights and complaints under the Processor BCR and how to contact us.

Applicability and scope

Introduction

Accenture's Processor BCR apply to Client Personal Data processed by Participating Entities where they act as a Data Processor for services we provide to Clients. Accenture's Processor BCR do not apply to Personal Data processed by Accenture as a Data Controller for our own purposes such as recruitment, employment or marketing.

The Processor BCR also govern the circumstances in which one Participating Entity acting as a Sub processor processes Client Personal Data on behalf of another Participating Entity acting as the Data Processor.

The Processor BCR require all Accenture Participating Entities and their Employees who collect, use and store Client Personal Data to:

a) understand their responsibilities under the Processor BCR when processing Client Personal Data and comply accordingly.
b) respect the Client's specific instructions for processing their Client Personal Data in accordance with each Client Service Agreement; and
c) understand how to respect and manage Individual Rights in relation to their Personal Data when helping Clients to manage these rights or assist individuals exercising their third-party beneficiary rights.

The Client must decide whether the Processor BCR apply to all Client Personal Data processed on its behalf by Accenture irrespective of origin, or whether it only applies to Client Personal Data subject to EEA law.

Accenture entities and affiliates

Accenture has offices and operations throughout the world. Client Personal Data may be transferred or be accessible throughout Accenture's global business and between our entities and affiliates unless otherwise agreed between Accenture and a Client or as required by data localisation laws. For a full list of Accenture Participating Entities and their locations, please click here or email DataPrivacyOfficer@accenture.com.

Description of Cross Border Transfers: categories of individuals, categories of Client Personal Data and processing, purposes, recipients, countries

The table in Annex 2 sets out (i) the categories of individuals we generally process information about, (ii) the categories of Client Personal Data we may process about them, (iii) the associated processing and purposes; and (iv) information about data importers and exporters and the countries where the processing may take place.

How we make our Processor BCR binding

The Processor BCR are made binding on Participating Entities and relevant Accenture Employees through the following means:

Intercompany Agreement – Accenture Privacy Agreement

Accenture's Processor BCR are made legally binding on our Participating Entities using an Intercompany Agreement -Accenture Privacy Agreement which can be found in Annex 4. No Cross Border Transfer will be made to an Accenture entity under the Processor BCR until they have signed the Accenture Privacy Agreement, are effectively and legally bound by the Processor BCR and can achieve compliance. However, we may use other transfer mechanisms to facilitate Cross Border Transfers, for example at the request of a Client or until an entity joins the Processor BCR. Changes to the Processor BCR Participating Entities list will be reported by the Data Privacy Team to all Participating Entities signed up to the Processor BCR and to the relevant Supervisory Authorities via the competent Supervisory Authority as part of the annual update.

Binding on Employees

The Processor BCR are made binding on Employees through a variety of measures, in particular, our Code of Business Ethics (COBE), our contracts of employment which include obligations to comply with Accenture's rules including policies and procedures, and our Client Data Protection Program. There are disciplinary procedures and sanctions for failure to comply with our COBE and the Processor BCR.

Data privacy and information security programs

As part of our data privacy program, Accenture has processes in place for managing our Processor BCR components, including compliance and training, monitoring and supervision, implementation of the Accenture Privacy Agreement across Participating Entities and specific information security practices. These programs are based on our policies which are binding. Accenture has a Data Privacy Team responsible for managing our Processor BCR. As part of our information security program, Accenture has a Client Data Protection Program to implement and manage data privacy and security requirements applicable to Client Personal Data. The Client Data Protection Program provides a standardized approach to implementing comprehensive and consistent controls to protect Client Personal Data. Accenture has a dedicated team responsible for managing the Client Data Protection Program.

Client Service Agreements – contracts

Client Service Agreements between Accenture and our Clients will include the relevant contractual provisions for the protection of Personal Data as required by Applicable Data Privacy Laws such as the EU Data Privacy Laws. Personal data protection terms and conditions can also be included in other Client related project documentation, user agreements or "Terms of Use" applicable to a project, platform, tool, or application (collectively known as "Client Service Agreement(s)" for the purposes of the Processor BCR). These Client Service Agreements will include specific references to the mechanism used to protect Cross Border Transfers of Personal Data, including the use of these Processor BCR, or other mechanisms approved between Accenture and the Client. When the processing of Client Personal Data relies on the Processor BCR, it will be clearly stated in the Client Service Agreement as a reference or an annex (as an electronic link or, upon request, the actual document).

Clients and data subjects can then enforce the Processor BCR against any relevant Participating Entity for breaches it has caused of the Processor BCR and of the Client Service Agreement relevant for the data subject affected. This includes the right to enforce the Processor BCR against the relevant EU based Participating Entity contracting directly with the Client even if the breach may have been caused by a Participating Entity

outside the EEA or a non-EEA third party Sub processor (e.g., operating under a separate contractual agreement for the purposes of onward transfer arrangements).

Accenture has accounted for how it manages these enforcement rights within our Accenture Privacy Agreement. Accenture has appointed a specific entity (Accenture Global Holdings Limited) based in the EEA as our Data Privacy Administrator to act on behalf of all Accenture Participating Entities (EEA/non-EEA) for the purposes of the Processor BCR. The Data Privacy Administrator is responsible for taking necessary action to remedy the acts of other Participating Entities outside the EEA and for breaches by external Sub processors outside the EEA and to pay any damages as a result of violations of the Processor BCR.

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

If a Client can demonstrate that it has suffered damage and can establish reasonable facts which show it is likely that the damage has occurred because of a breach of Processor BCR, to discharge itself from the liability for the damage, it will be for the EEA contracting Participating Entity and/or the Data Privacy Administrator:

- to prove that the Processor BCR Participating Entity outside of the EU or the external Sub processor was not responsible for the breach of the Processor BCR giving rise to those damages, or
- to prove that no Processor BCR breach never occurred.

If the contracting Participating Entity, as per the Client Service Agreement, can prove that neither it nor any Participating Entity/Entities outside the EEA nor any non-EEA external Sub processor is responsible for the breach, it may discharge itself and the other Participating Entity/Entities from any responsibility/liability.

Accenture's Processor BCR obligations

To protect Client Personal Data, Participating Entities and their Employees comply with the following obligations which are appropriately reflected in our core Client Data Protection Program and supporting procedures, controls and guidance. Accenture Participating Entities and Employees who access, collect, delete, retrieve, store, transfer or otherwise use Client Personal Data for any purpose, are "processing" that data and are responsible for understanding how data privacy impacts their role and their use of Client Personal Data and comply accordingly using the data privacy resources Accenture provides.

One - Being transparent and fair: Accenture has an obligation to assist Clients to comply with the law

Accenture and our Sub processors have a general and reasonable obligation to help our Clients comply with Applicable Data Privacy Laws and enable our Clients to be fair and transparent with individuals. Accenture will be transparent with Clients about our processing and sub processing activities so Clients can provide individuals with information (for example in a data privacy notice or privacy statement) about how their Personal Data will be processed by the Client and by us, on behalf of the Client.

An individual has the right to know about the Client's processing of their Client Personal Data and to verify whether that processing is lawful. Clients primarily provide this information to individuals directly, subject to Applicable Data Privacy Laws. Accenture will provide this information to individuals only when directed to do so by a Client in accordance with the requirements specified in an applicable Client Service Agreement.

Two - Purpose Limitation: Accenture has an obligation to process Client Personal Data according to Clients' instructions and the terms of the Client Service Agreements

Accenture will process Client Personal Data for specified purposes, in accordance with Client instructions and the terms of relevant Client Service Agreements,. In the event Accenture cannot comply with a Client's instruction, we will inform the Client (unless prohibited by law), who is entitled to suspend a Cross Border Transfer, process a change order and/or amend or terminate the Client Service Agreement.

When a Client Service Agreement ends, and/or the provision of some services ceases, Accenture and our Sub processors will follow Client instructions (as per the terms of the

Client Service Agreements) on deletion, return or onward transfer to a new processor/Sub processor. As applicable:

a) we will delete or return all copies within an agreed timeline and certify to the Client that we have done so, unless local laws and/ or contractual/other requirements prohibit the return or deletion of the Client Personal Data. Accenture warrants that it will continue to ensure compliance with the BCRs and will only process it to the extent and for as long as required under that local law and/ or Client Service Agreement and in a non-identifiable format;
b) in the event we retain the Client Personal Data, Accenture will inform the Client, keep the data confidential and will no longer actively process the Client Personal Data upon termination of the Client Service Agreement and/or we no longer provide those services, unless the terms of the Client Service Agreement include provisions for processing the data in a non-identifiable format.

Three – Data Quality: Accenture and our Sub processors have a general obligation to help Clients comply with the requirements to update, correct or delete Client Personal Data

Accenture and our Sub processors carry out reasonable and agreed measures (as per Client Service Agreements) to help Clients have their Personal Data updated, corrected, deleted, destroyed, pseudonymized, anonymized or aggregated where necessary and where required in accordance with legal/regulatory specified retention requirements. Where the Client Personal Data have been disclosed to several Participating Entities, Accenture and our Sub processors will inform those entities of the changes required, in particular in situations where identifiable Client Personal Data is no longer relevant to the processing.

When Accenture is asked to delete or destroy Client Personal Data, there are procedures for the secure disposal of such Client Personal Data in line with our security procedures.

Four - Individual Rights: Accenture has an obligation to help our Clients respect Individual Rights

Accenture and our Sub processors will use appropriate technical and organizational measures to help Clients fulfill their obligations to respect individuals' exercise of their Individual Rights, as far as it is reasonably feasible for us to do so. We provide our Clients with relevant information to help them comply with their obligations. We pass on individuals' requests to our Clients without responding to them unless this is an agreed service included in our Client Service Agreement. The extent to which we facilitate individuals' requests on behalf of Clients is determined by Clients. The arrangements we put in place vary according to the needs of each Client.

Five – Third Party Beneficiary Rights: Accenture has an obligation to facilitate these rights

Individuals have certain rights in relation to Accenture's obligations to comply with the terms of the Processor BCR. These are known as third party beneficiary rights. These rights apply when the Processor BCR are in place, irrespectively of the processing occurring outside the EEA or in a country which is not recognized as being an adequate jurisdiction. Individuals can enforce the Processor BCR against any relevant Participating Entity for breaches it has caused of the BCR and of the Client Service Agreement relevant for the data subject affected. This includes the right to enforce the Processor BCR against the relevant EU based Participating Entity contracting directly with the Client even if the breach may have been caused by a Participating Entity outside the EEA or a non-EEA third party Sub processor (e.g., operating under a separate contractual agreement for the purposes of onward transfer arrangements).

Individuals can take action directly against Accenture, if we fail in our obligations to:

a) respect Clients' instructions with regard to processing their Personal Data including Personal Data Cross Border Transfers outside the EEA.
b) implement appropriate technical and organizational security measures.
c) notify Clients about Personal Data Breaches.

d) put in place the necessary conditions and liability provisions to ensure the obligations set in the Processor BCR are flown down when engaging Sub processors either within or outside of Accenture.
e) provide reasonable assistance to Clients to comply and demonstrate compliance with Applicable Data Privacy Laws such as facilitating Individual Rights.
f) make the Processor BCR and its Annexes easily accessible to individuals (published on the acccenture.com site).
g) enable individuals to make complaints to Accenture, the Supervisory Authorities and/or courts (click here for more information in our "Managing claims, complaints or enquiries" section below).
h) cooperate with the Supervisory Authorities.
i) be transparent where national legislation prevents Accenture complying with the Processor BCR.
j) ensure that individuals can exercise their rights as third party beneficiaries in relation to the processing of their Personal Data and be entitled to remedies available under the BCR and Applicable Data Privacy Laws in respect of a given breach.

Individuals have the right to take legal action, via the relevant courts under applicable EU Data Privacy Laws, for any breach of their third-party beneficiary rights, including the right to lodge a complaint before the Supervisory Authority, obtain redress and where appropriate receive compensation for any damage (this may include material harm and distress), where required at law.

Accenture has accounted for how it manages these enforcement rights within our Accenture Privacy Agreement. Accenture has appointed a specific entity (Accenture Global Holdings Limited) based in the EEA as our Data Privacy Administrator to act on behalf of all Accenture Participating Entities (EEA/non-EEA) for the purposes of the Processor BCR. The Data Privacy Administrator is responsible for taking necessary action to remedy the acts of other Participating Entities outside the EEA and for breaches by external Sub processors outside the EEA and to pay any damages as a result of violations of the Processor BCR.

Accenture has addressed liability within our Accenture Privacy Agreement that includes provisions which deal with how Accenture assigns responsibilities, remedies and liabilities under the Processor BCR.

The Processor BCR confer rights to individuals to enforce as third party beneficiaries the rights stated section 5 a) to i) of these Processor BCR in case the individual cannot bring a claim against the Data Controller because the Data Controller has factually disappeared or ceased to exist in law or has become insolvent (applies where as a result of the insolvency arrangement (under applicable Local Data Privacy Law), they have become incapable of fulfilling their legal obligations as a Data Controller), unless any successor entity has assumed the entire legal obligations of the Data Controller by contract of by operation of law, in which case the individual can enforce their rights against the successor entity.

The Processor BCR are published on the accenture.com website. Our Clients have their own obligation to provide a copy of the Processor BCR and our service agreements (without proprietary, commercially sensitive or confidential information, as agreed in the relevant Client Service Agreement) to individuals upon request.

Six – Managing claims, complaints or enquiries (requests): Accenture has an obligation to handle some complaints directly

Dealing with requests on behalf of Clients

Accenture will inform Clients about any claims, complaints or enquiries made to us or our Sub processors which relate to the Client, or their Client Personal Data processed by Accenture, without undue delay, except where we have agreed to handle such matters on behalf of Clients. In these instances, we follow our Client's instructions and the terms of the Client Service Agreement.

Dealing with requests directly

In the event a Client organization no longer exists, or becomes insolvent, which applies also where, as a result of the insolvency arrangement under Applicable Data Protection Laws and Local Law, they have become incapable of fulfilling their legal obligations as a Data Controller, Accenture will handle individuals' complaints directly unless another entity has assumed the legal responsibilities of the Client. The handling of other requests and the return or destruction of the Personal Data concerned will be determined on a case-by-case basis depending on the terms agreed under the Client Service Agreement and the requirements of Applicable Data Protection Laws and Local Laws. For situations such as these, Accenture relies on our own procedure, as outlined below.

Format: All requests should be made in writing, and preferably 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 enable the request to be routed correctly.

Individuals will be asked to provide some of their Personal Data necessary to deal with their request, including to enable proper identification, possibly through a government issued ID.

Timeline: Requests are dealt with on a case-by-case basis and every attempt is made to resolve these as quickly as possible. For most complaints, Accenture will respond within one month of receipt or within specified timeframes (if shorter than one month) under Applicable Data Privacy Laws excluding the time it takes to verify an individual For some complaints, Applicable Data Privacy Laws allow Accenture an additional period of time to

respond (this can be no longer than two months but may be less depending on the Applicable Data Privacy Laws). Taking into account the complexity and number of the requests, within one month of receipt individuals will be made aware of Accenture's delayed response time and the reasons why.

Complaints and claims

Resolving a Complaint: Where a specific complaint is justified, Accenture and, where relevant, our Sub processors will 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 Processor BCR, our policies or Applicable Data Privacy Laws and regulations. Any action taken by Accenture will be in accordance with any applicable national laws and regulations, including but not limited to employment laws.

Escalating a Complaint: We encourage and welcome individuals to come to Accenture first to seek resolution of any request. If they are dissatisfied with the initial outcome, the matter will be escalated to the Senior Director, Global Data Privacy (Director) and Data Privacy Officer (DPO) for re-review.

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 States Supervisory Authorities is available here.

Making a claim: Individuals can also make a claim against Accenture via a competent court subject to local laws. The competent court is recognised as being in the member state of the European Union where the: individual (habitually) resides; individual's place of work is located; alleged infringement took place; or relevant Accenture Data Processor or the Client has an establishment. It is up to the individual to decide which competent court they would look to register a claim with. Accenture has the right to object to claims brought by the individual, where we are legally permitted to do so.

Record keeping and evidence

Accenture maintains records about requests in accordance with a Client's instruction or as agreed under Client Service Agreements and/or any applicable law requirements. Where appropriate, Accenture will also rely on its Retention Policy. 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 our own compliance purposes. In relation to Individual Right requests, if an individual escalates their request or complaint to a Supervisory Authority or engages in legal proceedings directly against Accenture, we will also maintain records.

Seven - Protecting Client Personal Data: Accenture and our Sub processors have an obligation to implement appropriate technical & organizational measures to protect Client Personal Data

General arrangements

Accenture maintains organizational, physical, and technical security measures for the Client Personal Data we hold and process through our multidisciplinary approach to security as set out in our Client Service Agreements. These measures are managed by the information security team which monitors and protects Accenture's overall technology environment. The team is structured as follows:

a) Client Data Protection Team which governs the stewardship of Client Personal Data and Client systems entrusted to Accenture
b) Risk Management Team which regularly monitors and assesses our information security risk position
c) Training and Awareness Team which manages on-going awareness communication campaigns and a mandatory training curriculum
d) Cyber Incident Response Team (CIRT) which manages the remediation of events and necessary corrective actions.

Accenture implements security measures as specified in Client Service Agreements and as required to at least meet the requirements of the Client's applicable law. Accenture and the Client would need to agree parameters (security measures and applicable costs) where applicable legal requirements go beyond the scope of technical and organizational measures generally conferred upon Data Processor. Accenture's Client Data Protection Program provides Client engagement teams with a structured approach to manage risks relative to the categories of Client Personal Data being processed and the type of processing through a set of management processes, controls, metrics and policies designed to address the risks. The risks are generally defined as accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to data.

Where applicable and if specified in our Client Service Agreement, Accenture also adopts or follows relevant security standards or certifications such as ISO 27001 as part of our information security practices.

Our Sub processors will have their own organizational, physical and technical measures to protect Client Personal Data and meet applicable legal requirements.

Personal Data Breaches

Accenture has procedures in place for identifying, managing and responding to Personal Data Breaches, understood as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. Instances of reasonably suspected or known Personal Data Breaches where there may have been inappropriate access to or an unauthorized disclosure of Client Personal Data must be reported promptly to the Accenture Security Operations Center (ASOC). All Employees are required to follow our security instructions. As part of our breach response management, our investigation teams provide forensic analysis and use relevant tools and intelligence to defend against malicious activity. There are internal procedures for informing Client account management teams, senior Client Data Protection Program and Data Privacy Officer Network and other relevant parts of the business about the incident.

There are procedures for reporting breaches externally to Clients based on the requirements agreed to within service agreements and of applicable legal including the GDPR. The information is provided without undue delay after becoming aware of any Personal Data Breach and includes details relevant to the breach, in compliance with applicable legal reporting requirements (for example, timeframe for notifying a breach, type of breach, number of individuals, types of Client Personal Data). There are also procedures for notifying other relevant bodies about breaches when legally required to do so in certain jurisdictions or when Accenture and/or the client considers it appropriate.

Accenture has arrangements with our Sub processors to inform us/our Clients of any Personal Data Breaches without undue delay after becoming aware of any Personal Data Breach and in accordance with the terms set out in our Client Service Agreements.

Accenture maintains a record of Personal Data Breaches which includes details about the incident. Accenture will make relevant information available to the applicable Client (as per Client Service Agreements and relevant legal requirements) and to the Data Controller supervisory authority.

Arrangements with Sub processors and other third parties

Accenture recognizes that adequate security is important where it arranges for external service providers (also known as “Data Processor” but defined as Sub processors for the purposes of Client Service Agreements) to process Client Personal Data as part of the services we deliver to Clients. Participating Entities will enter into contractual arrangements with all our external service providers who act as Sub processors to process Client Personal Data pursuant to a Sub processor arrangement, in compliance with any specific obligations, relevant security provisions and requirements as per any applicable data privacy laws. This includes when one Accenture entity processes Client Personal Data

on behalf of another Accenture Participating Entity pursuant to the Accenture Privacy Agreement.

These contractual arrangements will usually include obligations (including those required by law) including:

(i) a requirement to process Client Personal Data according to the documented instructions of the Accenture entity which is the processor and the client 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 Client Personal Data)

(iv) an obligation on the Sub processor to:

a) implement appropriate technical and organizational measures to protect the Client Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing and security requirements under applicable laws

b) respect the conditions of the Processor BCR for engaging another Sub processor

c) provide reasonable cooperation and assistance to the relevant Participating Entity/Entities to allow Clients and individuals to exercise their rights under the Processor BCR

d) assist the Client and the Participating Entity/Entities to comply with obligations to implement technical and organisational security measures, notify Personal Data Breaches, perform data protection impact assessments or prior consultations

e) provide reasonable cooperation to the Participating Entity/Entities and Client so they can demonstrate their compliance with all obligations – this includes, for example, the right of audit and inspection

f) make reasonable efforts to maintain the Client Personal Data so that they are accurate and up to date at all times

g) return or delete the data at the request of the Participating Entity and/or Client, unless required to retain some of the data as per contractual or legal requirements, and

h) maintain adequate confidentiality arrangements and not disclose the Client Personal Data to any person except as required or permitted by law or by any agreement between the Participating Entity and the Sub processor or with the Participating Entity's written consent.

If Sub processors are located in countries outside the EEA and they have access to or otherwise process Client Personal Data that is subject to EU Cross Border Transfer requirements, the contracts with such Sub processors shall include an EU approved mechanism for allowing such Personal Data transfers (adequacy decision, legally binding instrument between public authorities, binding corporate rules, standard data protection clauses adopted by the EU Commission, standard contractual clauses adopted by a supervisory authority and approved by the EU Commission, approved code of conduct together with binding commitments or approved certification mechanisms approved by EU Member states or exceptionally one of the specific derogations stated under EU Applicable Data Privacy Law).

Any use of Sub processors (internal or external) is arranged with the prior written authorisation of our Clients and in accordance with the terms specified within our Client Service Agreements covering authorizations for general or specific use of Sub processors. As set out in our Client Service agreements, notification of additional or replacement Sub processors is made by Accenture in a timely manner to allow Clients primarily to approve, raise any concerns, objections or where any agreement cannot be reached terminate the Client Service Agreement prior to any transfer of Personal Data to the new Sub processor. When Accenture engages Sub processors, we flow down the same or equivalent data security obligations as set out between Accenture and the Client in the Client Service Agreements.

Eight - Cooperation: Accenture has an obligation to cooperate with our Clients

Accenture and our Sub processors have an obligation to cooperate and assist our Clients to comply with data privacy laws, for example, by facilitating compliance with regulatory requirements and in accordance with our Client Service Agreements. To meet this obligation, Accenture takes into account measures such as data protection by design and default where possible, and Accenture cooperates and assists Clients during investigations or inquiries by Supervisory Authorities. Accenture will do so in a reasonable time and to the extent that this is reasonably possible. Accenture will inform the Client if in our opinion a Client instruction infringes relevant data privacy laws. Providing such information does not create an obligation on Accenture to provide legal or other regulatory advice to the Client and, subject to the applicable Client Service Agreement, Accenture should be entitled to suspend the execution of such an instruction until it is confirmed or changed by the Client.

Nine - Cooperation: Accenture has an obligation to cooperate with Supervisory Authorities

Accenture and our Sub processors have an obligation to cooperate with and to accept to be audited by the Supervisory Authorities competent for the relevant Data Controller, taking into account the advice and abide by the decisions of these Supervisory Authorities on any issue related to these Processor BCR.

Ten - Evidence: Accenture has an obligation to provide Clients with information to demonstrate compliance

Accenture maintains a written record, including in electronic form, of the data processing activities we carry out on behalf of our Clients and, subject to the terms of our Client Service Agreements, we have an obligation to provide Clients with information which demonstrates compliance with our data privacy obligations in relation to these activities; including compliance through audit and inspection. This record shall be made available by Accenture to the Supervisory Authority of the Data Controller upon request and shall contain: the details of the Data Processor and Data Controller and, where applicable their representative; the categories of processing carried out on behalf of each controller; where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the corresponding safeguards for such transfers ; and applicable technical and organisational security measures.

Accenture and Clients generally negotiate audit terms including the appointment of auditors, the agreed scope and parameters as part of the Client Service Agreements. Clients will be made aware of the audit scope and parameters in relation to relevant Sub processors. (See section on Audits for more information).

Eleven – Ensuring compliance with Cross Border Transfers requirements

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

Accenture has guidance in place to ensure that appropriate safeguards (including contractual arrangements where needed) are put in place for Cross Border Transfers of Personal Data to countries which do not have Applicable Data Privacy Laws or whose laws do not provide a level of protection which corresponds to the standards recognized by or offered within the EU Data Privacy Laws. This guidance includes information on when to apply the correct safeguards and contractual arrangements before any such Cross Border

Transfers take place. This includes assessments of Local Laws and practices prior to the transfer taking place (including data in transit) in order to determine to what extent European Essential Guarantees are respected. The Participating Entities may only use the Processor BCR as a tool for Cross Border Transfer where this assessment has occurred.

If Accenture concludes that an adequate level of protection for Personal Data cannot be guaranteed in the third country concerned, the data exporter in a Member State, if needed with the help of the data importer, shall assess and define supplementary measures to ensure a level of protection which is essentially equivalent to that in the European Union. Where effective supplementary measures could not be put in place, the Cross Border Transfers at stake will be suspended or ended.

Accenture has put in place procedures for implementing these safeguards to cover our day-to-day processing, for example, via these Processor BCR, or procurement contracts that include the relevant obligations conferred upon Sub processor as specified in Applicable Data 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 our BCR.

Accenture has a uniform approach towards the handling of Personal Data requests directed to any Accenture entity by any public authority or body that are massive, disproportionate and indiscriminate, whether such Personal Data relates to Client Personal Data, Employees, contractors, service providers, Clients or their customers.

Twelve - Accenture has an obligation to effectively comply with our Processor BCR

Accenture has internal arrangements to facilitate, audit and monitor compliance with our Processor BCR obligations, as described in Annex 1: How Accenture complies with our Processor BCR obligations. All individuals may rely upon these procedures and/or exercise their rights provided for in the Processor BCR.

If a Participating 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 Processor BCR obligations (or would have such an effect if the requirements were not imposed on the Participating Entity by law) it will inform the Accenture Data Privacy Team by email to DataPrivacyOfficer@accenture.com.

Consequences of Non-Compliance

We take compliance very seriously. If Accenture and our Sub processors fail to meet the data privacy obligations under the Processor BCR, we may cause risks or harm to individuals and Clients resulting in fines, penalties, criminal sanctions, loss of business and adverse publicity.

Contact Information

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

Annex 1: How Accenture complies with our Processor BCR obligations

Managing Data Privacy and information security

Data Privacy and information security are led by Managing Director level members of Accenture's leadership team.

Accenture has a Data Privacy Team led by the Senior Director, Global Data Privacy that defines, oversees, maintains and updates the data privacy program. Across the regions where we operate, we have a Data Privacy Officer Network which includes Data Privacy & Information Security Leads and which is supported by Geographic Compliance and Corporate Team, asset stewards and designated individuals within corporate functions each with specific responsibilities and accountability for data privacy management.

We also have a Data Privacy Officer (DPO) who reports into the Senior Director, Global Data Privacy, but also has the right to directly escalate issues to other senior leadership within Accenture, including board level, the Chief Compliance Officer and the General Counsel.

To help manage our information security program, Accenture has a global information security team led by our chief information security officer. Across our global organization we have a network of information security teams responsible for overseeing the use of technology to protect Personal Data, deploying risk management procedures to continually assess and monitor our information security risk position, managing Accenture's overall cyber incident responses and managing the appropriate information security training and communications.

Accenture has implemented a Client Data Protection Program that is part of Accenture's information security program to help secure the Client Personal Data and Client systems entrusted to us. Client accounts have defined roles with responsibility for Client Data Protection Program for that Client account. Teams collectively establish Client Data Protection Program processes and coordinate relevant Client Data Protection Program activities across all parts of the Client account. This includes conducting risk assessments and developing Client solutions that meet Client Data Protection Program controls, regulatory and Client requirements and managing those relevant controls applicable to the services provided. Key elements of our Client Data Protection Program include:

a) Senior level accountability for data protection and Clients' services where we have access to confidential business or Personal Data;
b) Security foundational training for Employees assigned to Client's engagement as part of the on-boarding process;

c) Clear documentation and communication of data protection requirements and function-specific training for Accenture people with access to confidential Clients' data;
d) Required controls for processing confidential data and enhanced controls for processing highly confidential business and Personal Data
e) Service specific controls for specific types of work for particular Clients' engagements
f) Technology support and subject matter specialist support for project teams

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

Due to the global and complex nature of Accenture's operations, there may be several teams 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 Processor BCR

The Data Privacy Team is responsible for the overall management and supervision of the Processor BCR and coordinates with the relevant internal stakeholders and, where necessary, Supervisory Authorities.

The day-to-day responsibilities for different aspects of data privacy and security compliance and monitoring including providing guidance, interpreting requirements and providing support are shared across Accenture teams. The teams primarily involved include Data Privacy Team, information security team including Client Data Protection Program team, the Sales & Delivery Legal Team and compliance monitoring team. Any issues and reporting requirements which are specific to the Processor BCR will be sent to the Data Privacy Team, so they can accurately report relevant information to the competent Supervisory Authority.

Collectively, our teams' obligations are to:

a) enable routine monitoring and compliance with the Processor BCR, Applicable Data Privacy Laws and regulations at global, regional and country level
b) be responsible for maintaining the Processor BCR and modifying them when required to reflect regulatory changes, alterations to the Accenture group structure or any other changes which should be reflected within the Processor BCR.
c) record and track all changes and updates to the Processor BCR (Accenture Privacy Agreement, Disclosure Requests and routine reporting to the Supervisory Authorities) and the rationale for the updates and provide this information systematically to Participating Entities, our Clients and the Supervisory Authorities, as required or as part of our annual update.
d) maintain security controls which reflect the requirements of the Processor BCR.
e) maintain and continually develop audit controls for the Processor BCR.

f) communicate with the competent Supervisory Authority, our Clients and Participating Entities, if a proposed change to the Processor BCR either affects the level of protection offered by the Processor BCR or significantly affects the Processor BCR, in particular the binding nature, and

g) Accenture has an obligation to inform the relevant Supervisory Authorities of matters to the competent Supervisory Authority or other Supervisory Authorities, where necessary.

How Accenture supervises Processor BCR compliance

Accountability

Accenture Employees are:

(i) responsible and accountable for processing Client Personal Data in accordance with the Processor BCR, Client Service Agreements and Applicable Data Privacy Laws generally

(ii) required to comply with Accenture's relevant policies and guidance, including when processing Client Personal Data, and

(iii) expected to understand the data privacy requirements which have relevance to the Client Personal Data they process governed by Accenture 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 implemented 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 Code of Business Ethics, data privacy and information security training programs for all our Employees. Our Client Data Protection Program includes specific training applicable to delivery of Client services and a certification program for key Client Data Protection Program roles. Appropriate and timely training on the BCR will be provided to Accenture Employees that have permanent or regular access to Client's Personal Data and/ or who are involved in the collection of Personal Data or in the development of tools used to process Personal Data. Some training programs will be mandatory for certain roles. If required to do so, Accenture will provide the Supervisory Authorities with examples of our training program.

Record keeping and evidence

Accenture maintains records of our data processing activities and compliance and is prepared to show Clients, auditors, Supervisory Authorities, and other public authorities how we meet our record keeping obligations. These records are held and maintained by

different functions with regular reporting channels into the Data Privacy Team responsible for checking compliance with the Processor BCR and our 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 Data Privacy Laws

In addition to complying with the Processor BCR, each Participating Entity is responsible for taking such additional action as may be desirable or necessary to comply with Applicable Data Privacy Laws that may apply to the data and/or in the country where it operates. If Applicable Data Privacy Laws require higher level of protection for Personal Data, they will take precedence over the BCR. This will apply also in the event of a possible future conflict between new Local Law and the Processor BCR.

Upon the request of another Participating Entity or the Data Privacy Team, the Participating Entity in question will supply a copy of such Applicable Data Privacy Laws to the requesting party. In addition, to the extent that a Participating Entity from time to time adopts internal procedures designed to promote compliance with Local Laws, it will provide the Data Privacy Team with a copy of such procedures.

Audits

Accenture has a data privacy compliance audit program. The purpose of these audits is to assess our compliance with our policies, procedures and practices, Applicable Data Privacy Laws, and the Processor BCR.

Different aspects of our auditing program address data privacy compliance. Accenture has developed a series of audit controls against which to monitor our data privacy compliance. These controls cover full compliance with the obligations we make in the Processor BCR, our data privacy policies, procedures and processes and compliance with Applicable Data Privacy Laws. Accenture conducts regular data privacy audits, reviews and risk assessments. There are also regular information security audits and mandatory audits at least every 3 years for any standards or certifications we adhere to, for example ISO 27001.

There is an audit and risk assessment schedule for routine audits and where necessary, we will conduct an audit outside this schedule, under exceptional circumstances. Audits are generally conducted internally by our internal audit function, the Data Privacy Team, or externally by an organization specializing in audits.

In accordance with Applicable Data Privacy Laws and subject to reasonable security procedures, Clients may conduct an audit of our data processing activities and any facilities that are under our operational control, when the activities and facilities relate to the services we offer to those Clients. In these instances, Accenture and Clients generally negotiate audit terms including the appointment of auditors, the agreed scope and clearly defined parameters as part of Client Service Agreements, e.g., access to Accenture's shared services environments is often limited in order to protect the confidentiality of our Clients' data and avoid security risks.

Where Accenture is leveraging external hosting partners (such as public cloud service providers) as its Sub processors, Accenture and the hosting partners generally negotiate

a data processing agreement. These data processing agreements typically contain an audit provision whereby an independent third-party auditor will carry out at least one annual audit to inspect the compliance with the agreed data processing agreement.

Audits are generally conducted according to a mutually agreed processes designed to avoid disruption to the services and business generally, to protect the confidential information of Accenture, our Sub processors and other Clients and comply with relevant legal obligations. Clients will be made aware of the audit scope and parameters in relation to relevant Sub processors. The audits can be conducted by the Client, or an approved external auditor with the relevant qualifications and bound by a duty of confidentiality to conduct such audits.

In accordance with Applicable Data Privacy Law and subject to reasonable security procedures, Accenture and our Sub processors agree to be audited by competent Supervisory Authorities, including our Clients' competent Supervisory Authorities. The scope and parameters of such audits will be defined as and when such a request is made by the Supervisory Authorities. Accenture and our Sub processors will comply with such audits, subject to compliance with Local Laws as reasonably necessary to demonstrate compliance.

Accenture is committed to working in good faith to resolve a Supervisory Authority request through discussion and interaction. Nothing in the Processor BCR will be construed to limit any audit rights that a Supervisory Authority may have under Applicable Data Privacy Laws. In the event of any conflict between these Processor BCR and Applicable Data Privacy Law related to Supervisory Authority audit, the provisions of Applicable Data Privacy Law shall prevail.

The results of audits relating to the processing of Client Personal Data are made available to the DPO, Senior Director, Global Data Privacy, and any relevant Accenture function and geographic leadership, including relevant boards of directors. Upon request, relevant audit information will be made available to Supervisory Authorities and Clients (as per the terms of Client Service Agreements) as reasonably necessary to demonstrate compliance.

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

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

Violations of the Processor 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 Processor 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 Processor 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.

How Accenture cooperates with the Supervisory Authorities and Clients

Reporting matters to the competent Supervisory Authority

Routine reporting: Accenture will report routine updates to the Processor BCR with a brief explanation on reasons of update along with an updated list of Accenture Participating Entities as part of our annual update to the competent Supervisory Authority and in line with requirements specified in the section: Managing the Processor BCR. Where a modification to the Processor BCR would affect the level of protection offered under the Processor BCR, Accenture has an obligation to promptly communicate this to the Supervisory Authority.

Conflicts between Local Laws and the Processor BCR: Accenture has an obligation to inform the relevant Supervisory Authorities, namely the Supervisory Authority competent for the Controller and the Supervisory Authority competent for the Processor, of any conflict between Local Law requirements and the Processor BCR where this conflict would have a substantial adverse effect on Accenture's obligations under the Processor BCR.

Where a Participating Entity has reasons to believe that the existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the Controller or its obligations under the BCRs or Service Agreement, it will promptly notify this to the Controller which is entitled to suspend the transfer of data and/or terminate the contract, to the Privacy Administrator and to the relevant Supervisory Authority.

Accenture Participating Entities are required to report such conflicts to the Data Privacy Team as soon as they become aware. This includes any legally binding requests for disclosure of Client Personal Data to a law enforcement or other security agency.

Advice from the competent Supervisory Authority: Each Participating Entity will comply with advice from the competent Supervisory Authority on any issues relating to the Processor BCR. Any advice would be subject to legal review to consider any factors which inhibit the Participating Entity's ability to comply and where relevant, we would discuss alternative legal remedies with the Supervisory Authority.

Record of processing activities: Accenture will make our records of processing activities we conduct on behalf of Clients available to the competent Supervisory Authority on request.

Reporting matters to Clients

General reporting requirements: Participating Entities and our Sub processors will meet the reporting requirements under the Processor BCR, Client Service Agreements with our

Clients and Applicable Data Privacy Laws, including any relevant conflicts with Local Laws which may have a substantial adverse effect on our obligations under the Processor BCR.

Modifications to the Processor BCR: Accenture has the right to modify our Processor BCR, for example to reflect changes in Local Law or to our organizational structure. If a change materially affects the processing conditions to a lesser standard, Accenture shall inform our Clients in a timely manner allowing the Clients to object to the change, rely on an alternative Cross Border Transfers mechanism or exercise any rights to termination, dispute resolution or remedial action as outlined in individual Client Service Agreements, prior to the change taking effect.

Disclosure Requests: keeping Supervisory Authorities and Clients informed

Transfers of Personal Data by Accenture Participating Entities to any public authority cannot be massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society. All Accenture Participating Entities must report any such disclosure requests regarding Client Personal Data by a law enforcement authority or state security body to the Data Privacy Team.

Accenture will inform affected Clients and the competent Supervisory Authority of all such disclosure requests (unless we are prohibited or temporarily prevented from doing so under law provisions specifying confidentiality during the course of a law enforcement investigation). Any response to the request will be put on hold until the competent Supervisory Authorities for the Client and for the Data Processor have been informed about the request (including the data requested, legal basis for making the request, the identity of the requesting party and the response provided) unless we are prohibited from doing so. The Client is responsible for liaising directly with their competent Supervisory Authority regarding such requests.

The Data Privacy Team will keep a record of any such disclosure requests regarding Client Personal Data received by Accenture. These records should include details about the disclosure, the categories of data requested, the identity of the requestor) and any other relevant information (unless prohibited by Local Law to retain this information). The Data Privacy Team will provide the competent Supervisory Authority with an annual update of the records about requests that can be disclosed and will inform the competent Supervisory Authority about those cases subject to disclosure prohibitions as soon as such prohibition on notification are waived.

In those cases when notifications are prohibited, the Participating Entities shall use their best efforts to obtain the right to waive such prohibition in order to communicate as much information as possible and as soon as possible and will document their best efforts in order to be able to demonstrate that they did so.

Transfer Impact Assessments (TIA)

When Accenture, acting as Data Processor, acts as a data exporter of Personal Data from the EEA, Switzerland and the UK to another country that was not found to be adequate, Accenture performs a Transfer Impact Assessment (TIA) to identify any risk associated with the Cross Border Transfer (including the possibility of access requests by public

authorities) and to define supplementary measures to safeguard the Personal Data, if necessary. Where effective supplementary measures could not be put in place the Cross Border Transfers at stake will be suspended or ended, according to the specific terms stated int the Client Service Agreement.

The completion of the TIA – where an Accenture entity is the Exporter - is the responsibility of the Accenture team in charge of the specific Client Service Agreement or Cross Border Transfers. There is no need to repeat the assessment every time there is the same Cross Border Transfer of a specific type of EEA/UK/Swiss Personal Data to the same third country unless any changes in assessed circumstances (e. g. third countries legislation, etc.) has been made.
The TIA and, where needed, the decision on what supplementary measures to implement are documented and centrally stored by the Data Privacy Team and internally accessible. These will be made available to the Controller and to the competent Supervisory Authority on request.

National security laws Overview- "Country Transfer Risk Assessment"

The Data Privacy Team performs assessment of the legislative framework in relation to national security and surveillance laws and practices of certain countries. Such assessment aims to assess which appropriate safeguards, enforceable Individual Rights and effective legal remedies for data subjects exist when Personal Data subject to EU Data Privacy Laws, EEA, Swiss and/or the UK legislation is transferred to countries that have not formally been found "adequate" under the terms of the GDPR. These requirements were laid out by the European Court of Justice in its judgment in Case C-311/18 (also known as "Schrems II") of 16 July 2020 and were further interpreted by the European Data Protection Board Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of Personal Data.
The Country Transfer Risk Assessments are prepared by Accenture for the information of the Participating Entities and aim to support Client and eventual data exporters of Personal Data in satisfying themselves that the legislation of such countries enables recipients of Personal Data to comply with the data importers' obligations under the Standard Contractual Clauses or Processor BCR. The assessments do not replace the independent determination by the Client or other data exporter.

The Client is required, when acting as the data exporter, and where appropriate in collaboration with the data importer, to verify on a case-by-case basis whether the level of protection required by EU, EEA and Swiss law is respected in the third country concerned. Accenture is not responsible for the Client's determinations but will follow Clients' guidelines for the Cross Border Transfer to those countries, unless Accenture considers that an existing protection measure is not appropriate for a given country or transfer. In that case the provisions of the Client Service Agreement to supplement or protect Cross Border Transfers will apply, or Accenture might suspend the Cross Border Transfer of the services.

The Data Privacy Team keeps records of those Country Transfer Risk Assessments and reviews them periodically to identify any given significant change in the legislation that could require additional or different protection measures.

Annex 2: Categories of individuals, categories of Client Personal Data, purposes and processing, data importers and exporters, countries (separate document for review purposes)

Annex 3: Definitions (separate document for review purposes)

Annex 4: Intercompany Agreement – Accenture Privacy Agreement

This is an internal document which is made available as required but is not published on the Accenture.com website.