Annex 4: UK BCR 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 (UK BCR)

UK BCR (Binding Corporate Rules) are an UK mechanism to allow international transfers of personal data from the UK across Accenture's worldwide organization. They are legally binding and the Information Commissioner is responsible for their approval. Accenture entities signed up to the UK BCR comply with the same internal rules for processing personal data. Individuals' rights stay the same irrespective of which Accenture location they are processed. The UK BCR 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.

Code of Business Ethics (COBE)

Our COBE states that we operate with integrity and in an ethical manner. It is organized into six fundamental behaviours 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.

Data Controller

A data controller is specific to UK 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 UK 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 Market Unit. They also carry out tasks delegated by Accenture's Data Privacy Officer and act as the point of contact for the relevant data privacy regulators. The Data Privacy & Information Security leads are the first point of contact for local data privacy questions from employees.

Data Privacy Officer (DPO)

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 UK BCR commitments are based on this Policy.

Data Privacy Site

There is a dedicated website available to Accenture employees for data privacy resources and relevant information, news and updates (access is restricted to Accenture only).

Data Processor

A data processor is a term specific to UK data privacy laws and can be used in other data privacy laws. It is an organisation 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 the UK 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 UK GDPR.
>
> **Privacy Review:** a privacy review is not a mandatory requirement under the UK 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.

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 UK 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.

Data Transfers

Some data privacy laws have specific restrictions on transferring personal data outside a country or region's borders. If required, 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 organisation and to third party suppliers and vendors located outside the UK. UK data privacy laws, for instance, require that when such a transfer takes place, additional safeguards, for example, model clauses or UK BCR are put in place to protect the data.

Employee

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

EU BCR

Accenture's BCRs covering Data Transfers from the EEA and other jurisdictions (excluding exports of personal data from the United Kingdom which are governed by the UK BCRs).

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. Fines can run into hundreds of thousands of dollars (US $) for these types of non-compliances. The UK GDPR currently has significant consequences for non-compliance. These include:

Financial penalties: fines that in some instances are calculated based on revenue

Processing restrictions: an organisation 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

General Data Protection Regulation (EU GDPR)

EU GDPR is the "General Data Protection Regulation", (Regulation (EU) 2016/679) which applied from May 25th, 2018.

Geographic Compliance and Corporate Leads

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

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.

Individual Rights

Some data privacy laws such as the UK 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 UK BCR. That means someone who works for Accenture in a country with no privacy laws would have the same rights under our UK BCR as someone who works in a country with privacy laws. The UK GDPR includes a 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 UK 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 UK 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.

Information Commissioner

The Information Commissioner is the head of the UK's Information Commissioner's Office (ICO), the independent body set up to uphold information rights.

Intercompany Agreements (ICA)

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 UK 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 also need to meet additional requirements in order for the processing to be considered lawful.

For example, the UK 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,
- is necessary for the performance of a contract,
- is required to satisfy a legal obligation which the controller must comply with, or
- 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

Many 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 (internal access only).

Many privacy laws stipulate consent as one of the legal bases for processing personal data lawfully. For example, under UK 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.

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.

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 UK data privacy laws.

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 UK data privacy laws and in other countries with data privacy laws, is considered good practice.

Processing

Processing 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 UK 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.

UK Data Privacy Laws

UK Data Privacy Laws is a generic way of grouping together the UK GDPR and the UK Data Protection Act 2018.

UK GDPR

UK GDPR is the EU GDPR as it forms part of retained EU law (as defined in the European Union (Withdrawal) Act 2018).