ACCENTURE UK BCR - P SUMMARY

July3,2026

Accenture has implemented Binding Corporate Rules for Processors ("**EU BCR-P**") as an appropriate safeguard under applicable data protection legislation, ensuring a high and uniform level of protection for personal data processed within Accenture's multinational corporate group.

The EU BCR-P apply to Client Personal Data processed by Participating Entities acting as Data Processors, including subprocessing between Participating Entities. The EU BCR-P have been reviewed and approved by the competent supervisory authorities across the EU and are available at Binding Corporate Rules (BCR) | Accenture

To address transfers of personal data from the United Kingdom and processing subject to the territorial scope of the UK GDPR, Accenture has entered into a UK BCR Addendum to its approved EU BCR-P. The UK BCR Addendum is a **formal legal mechanism** that extends the application of the EU BCR-P accordingly. Together, the EU BCR-P and the UK BCR Addendum form **Accenture's UK Binding Corporate Rules for Processors** ("**UK BCR-P**"). Further information about the UK BCR addendum process is available on the UK Information Commissioner's Office ("ICO") website at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international transfers/guide-to-binding-corporate-rules/a-uk-bcr-addendum/

The UK BCR-P apply to transfers of personal data from the United Kingdom and to the processing of personal data relating to individuals in the United Kingdom by Accenture entities outside the United Kingdom, including where such processing falls within the territorial scope of Article 3 of the UK GDPR.

This **UK BCR-P summary** is intended to provide information to individuals whose personal data is processed under the UK BCRP, including information on applicable safeguards, data subject rights and how those rights may be enforced, and to provide relevant information to third-party data exporters relying on the UK BCRP.

Contact Details for Queries under the UK BCR-P (Data Subjects and Third-Party Exporters)	Individuals may exercise their rights or submit complaints by contacting Accenture Data Privacy Officer: **Email:** dataprivacyofficer@accenture.com Alternatively, individuals may contact the **UK Information Commissioner's Office** ("**ICO**"): https://ico.org.uk/make-a-complaint/ +44 303 123 1113 In addition, individuals have the right to seek judicial redress and, where applicable, compensation by bringing a claim before the UK courts against the Lead UK BCR

	Member, **Accenture (UK) Limited**, 30 Fenchurch Street, London, EC3M 3BD, for breaches of the UK BCR-P by any Accenture BCR Member or external sub-processors. For third-party data exporters relying on Accenture's processor Binding Corporate Rules, **equivalent rights and complaint mechanisms apply**, including the right to bring claims before the UK courts in relation to breaches of the UK BCR - P by the Lead UK BCR Member or any non-UK Accenture BCR Member, including sub processors. Further information, including the list of Accenture BCR Members and details of the complaint handling process, is available at: https://www.accenture.com/gb-en/about/binding-corporate-rules
Description of Data Transfers under Accenture's UK BCR (Data Categories and processing activities)	**Categories of Personal Data** • **Contact Information and Other Personal Information** – Name, all types of contact details (such as e-mail, phone numbers, physical address – contact details can be Business or Personal), gender, date of birth, place of birth, internal company employee or id numbers, marital/civil partnership status, domestic partners, dependents, disability status, emergency contact information, photograph, and images/footage captured on CCTV or other video systems, security pass information including photo and access rights, driver license number, car details and other necessary data for use of company cars (including clearing, damage events, insurances), investigations, complaints and grievances data, mergers and acquisitions data • **Bank Account Number** – Letters and/or numbers that form primary identifier of an account • **Credit Card Data** – Credit card number, cardholder name, expiration date or service code/CCV • **Personal Financial Data** – Financial/fiscal situation, credit reports, credit scores and fraud alerts • **Government Issued Personal Identifiers** – National Identifier, Social Security Number, Social Insurance Number, Driver's License Number, Passport Number • **Device Identifiers and Digital Identity Data** – such as serial numbers, unique device identifiers (UDIDs) for mobile phone IP address, MAC address, logs, or other unique identifiers as also included in

	network data • **Location Position Data** – Movement, GPS, GSM, WIFI, Bluetooth data • **Personal Life Data** – Lifestyle choices (e.g. smoking habits, exercise preferences), personal habits, and family situation. This could also include data that could be indicative of personal habits or interests like browsing data, purchasing data, social media, or usage data. • **Browsing Data** – IP address or similar identifier, user browsing history on websites and apps, including pages views, actions taken and pages viewed • **Purchasing Data** – data related to purchasing behavior and history, whether online or offline, for a variety of goods and services, including purchasing information (type of purchase, when, where price) and purchasing interests (related to future potential purchases) • **Social Media Data** – posts, photos, contacts and other content posted on social media, account details of users, metadata related to use of social media • **Usage Data** – data related to usage of platforms and services, such as times, quantities, patterns and behavior of use • **Consumer Profiles Including Marketing Profiles** – profiles of consumer or individual preferences and behavior aggregated together from one or more categories of data and sources of data including marketing preferences and profiles. • **Personal Data Subject to Media Attention** – Names and unpublished addresses/phone numbers of public figures, list of people with a specific condition or criminal charge. We may be required to process the following types of Sensitive Personal Data on behalf of our clients because they have a valid legal basis to process such information. We are likely to process such information in relation to services such as HR & Payroll or Financial Crime Prevention, for example. • **Criminal Data** ¬– Personal Data relating to criminal convictions and offences • **Health Data** – Data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the individual

	• **Race or Ethnicity Data** – Self-identification data items in which residents choose the race or nationality with which they most closely identify • **Genetic Data** – Data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question • **Biometric Data** – Personal Data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images, iris scans, fingerprints or dactyloscopic data • **Political Views** – Data that identifies affiliation or support with a political party or ideology • **Religion** – Data that identifies affiliation or support with a religious organization • **Trade Union Membership** – Data that ties an individual to membership with a Trade Union • **Sexual Orientation** – Data identifying preference of sexual partners • **Other** types of Personal Data not specified here but unique to client processing of Personal Data. More information about **categories of client personal data** can be found in ANNEX 2 of EU BCR-P: Binding Corporate Rules (BCR) | Accenture **Types of Processing** For the purposes of the UK BCR-P, “processing” has the same meaning as under Article 4(2) UK GDPR and includes, for example: • collection, recording, organisation and storage of personal data. • use, consultation and retrieval. • disclosure by transmission, transfer or otherwise making data available. • alignment, combination, restriction, erasure or destruction. The UK BCR-P apply to all categories of personal data and to all processing activities described in this summary, whether carried out by automated or manual means.

	More information about **types of processing** can be found in ANNEX 2 of EU BCR-P: Binding Corporate Rules (BCR) | Accenture
List of countries where BCR Members are located / data is transferred to	**A list of Accenture BCR Members and the countries in which they are established**, including locations relevant to processing on behalf of Third-party Exporters, is available at: https://www.accenture.com/gb-en/about/binding-corporate-rules
Rights of Relevant Data Subjects (including third-party beneficiary rights)	Accenture's UK Binding Corporate Rules for Processors ("UK BCR-P") confer **legally binding and enforceable third-party beneficiary rights** on Relevant Data Subjects. These rights arise directly from Accenture's commitments under the UK BCR-P and are **in addition to** the statutory rights available under the UK data protection framework. **Third-party exporters** relying on Accenture's Processor Binding Corporate Rules are granted legally enforceable third-party beneficiary rights. Data subjects can then enforce the UK BCR-P against any relevant Participating Entity for breaches it has caused of the UK BCR-P. The Lead UK BCR Member agrees to be fully liable to Relevant Data Subjects, to the ICO, and third-party exporters for all material and non-material loss and damage caused directly or indirectly by any Non-UK BCR Member's breach of this UK BCR , including where caused by any Non-UK BCR Member's Processor. There are the two types of third-party beneficiary rights for data subjects under a UK BCR-P, that are enforceable directly against the Processor and; enforceable against the Processor in case the data subject is not able to bring a claim against the Controller (e.g. where a Controller has factually disappeared or ceased to exist in law). In particular: • Duty to respect the instructions from the Controller • Duty to implement appropriate technical and

	organisational security measures and duty to notify any personal data breach to the Controller (Arts.28.3(a), 28.3(g) and 29) • Duty to respect the conditions when engaging a sub-processor either within or outside the group (Arts.28.2, 28.3(d), 28.4, 45, 46 and 47) • Duty to cooperate with and assist the Controller in complying and demonstrating compliance with the law such as for answering requests from data subjects in relation to their rights (Arts.28.3(e), 28.3(f) and 28.3(h)) • Art.47(2)(g) - Easy access to the UK BCR Summary • Art.47(2)(i) - Right to complain through internal complaint mechanisms • Art.47(2)(e) & (f) - Liability, compensation and jurisdiction provisions • Art.47(2)(l) - Duty to cooperate with the Information Commissioner • Art.47(2)(m) - National legislation preventing respect of UK BCRs • Right to the list of entities bound by the UK BCRs.