ACCENTURE UK BCR-C SUMMARY

July 3,2026

Accenture has implemented Controller Binding Corporate Rules approved for the European Union ("**EU BCR-C**"), which constitute an internationally recognized data transfer mechanism designed to ensure a high and consistent level of protection for personal data within multinational organisations. **Accenture's EU BCR-C** is publicly available at: Binding Corporate Rules (BCR) | Accenture

To address transfers of personal data from the United Kingdom, Accenture has entered into a UK BCR Addendum to its approved EU BCR-C. The UK BCR Addendum is a **formal legal mechanism** that extends the scope of the EU BCR-C to cover transfers of personal data originating from the United Kingdom.

Taken together, the EU BCR - C and the UK BCR Addendum form **Accenture's UK Controller Binding Corporate Rules** ("**UK BCR-C**"), providing a unified and robust framework for intragroup transfers of personal data from both the EU and the UK.

The UK BCR-C apply to:

- Transfers of personal data from the United Kingdom to other Accenture entities located outside the UK; and
- Processing personal data relating to individuals in the UK by Accenture entities outside the UK, where the UK GDPR applies.

This includes situations where processing falls within Article 3 of the UK GDPR, such as when Accenture: (i) offers goods or services to individuals in the UK, or (ii) monitors the behavior of individuals in the UK, to the extent such monitoring takes place in the UK.

Contact Details for Queries under the UK BCR-C	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 Claims for redress or compensation may be brought before the UK courts, against the Lead UK BCR Member (**Accenture (UK) Limited**, 30 Fenchurch Street, London, EC3M 3BD) for redress and compensation for breaches of the UK BCR-C by any BCR Member. The courts of England and Wales, Scotland and Northern

	Ireland all have non-exclusive jurisdiction over any claim in connection with this UK BCR Addendum (including non-contractual claims). Relevant Data Subjects may bring a claim against any BCR Member in connection with this UK BCR Addendum (including non-contractual claims) in any court in any country with jurisdiction to hear the claim. Full details, including the list of BCR Members and the complaints procedure, are 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** The UK BCR-C cover a broad range of personal data categories, including data relating to: **Personal details [employment context] -** Name, preferred pronoun, all types of contact details (such as e-mail, phone numbers, physical home and place of work address), gender, date of birth, place of birth, national identification number, social security number and health insurance number, insurance information, internal company employee or id numbers, marital/civil partnership status, domestic partners, dependents, disability status, emergency contact information, ethnic origin, minority flag, biometric data (such as facial images, voice recognition/patterns, iris patterns or fingerprints), photograph, and images/footage captured on CCTV or other video systems, footage/voice recordings captured during events/sessions (including recording of virtual or live workshops or similar events), smart building controls and metric systems used for data analytics, driver license number, car details and other necessary data for use of company cars (including clearing, damage events, insurances), government-issued ID number; military status and rank; emergency contact details; usage/account details of cards for restaurants and vending machines; information obtained through the use of surveys; investigations, complaints and grievances data including as part of the business ethics line; mergers and acquisitions data, work anniversary. **Personal details [clients & prospects]** - Name, all types of contact details (such as salutation, job title, e-mail, phone

	numbers, physical home and place of work address), contact preferences, preferred language for communications, marketing preferences, minority flag data relating to goods and services provided or obtained, relationship with Accenture [prospect, client, alumni now client]; data related to events [invitations, attendance, relevant costs]. **Personal details [vendors, service providers, suppliers, payees and intermediaries, legal services data]** – Name, all types of contact details (such as salutation, job title, e-mail, phone numbers, physical home and place of work address); preferred language for communications; data related to invitations for business trips or other business events (e.g., itinerary, costs); entity tax identification number and commercial registry registration number; entity nationality; entity bank details and payment related information, bill to and ship addresses, billing currency; VAT (or equivalent) number; customer/vendor/supplier number or other unique identifier; country registration number, where applicable; information derived from the deployment and use of information systems and tools including from third parties; records related to the provision and management of products orders or returns, provision of services, accounts and internal **Leaves of absence -** Vacation, statutory leaves, and voluntary leaves (including maternity and paternity leaves sabbaticals), justification for paid absences (including education, family events, social activities, children and other dependents' care). Data relating to administration or leave (including start date, end date, temporary suspension), illness including accidents at work and occupational health (in accordance with local law). Dates (beginning, end and duration). **Pension records -** Monthly pension, yearly pension, capital sums, deferred compensation sums, type of pension plan; other data related to pension fund (including enlistment and discharges, contribution data and insurance period in the statutory Social Security). **Position and contractual information -** Description of current position, job title, corporate status, career level, management category, job code, job function(s), legal

	employer entity, location, Accenture contact(s), employee identification number, terms and conditions of employment or contract, membership of the board of directors, information on extent of shareholding, work history, hire/re-hire and termination date(s) and reason, information from exit interviews/termination documents, length of service, executive management responsibility, trade union membership, retirement eligibility, promotions and disciplinary records, date of transfers, and reporting manager(s) information. **Work location & relocation -** Working address, place of work (including work place office, home office, shared desk, external work), workplace indicator, work location code, branch office, sales office, building, room, locker, relocation information (including international assignment flag, assignment data and dates, current assignment, future assignment, country, hypotax, tax reconciliation, foreign tax); employment permits (including date); visa country, visa expiration date, mobility preferences, termination date and reason code; assignment responsibility, assignment job title, tasks; employee's willingness to travel or relocate. **Talent management information –** Details contained in letters of application and resume/CV or other provided documents (previous employment background, education history, professional qualifications, any technical specialisations or qualifications, trade licenses, language and other relevant skills, certification, certification expiration dates), information of recruitment interviews/check lists, legal prerequisites for employment, information necessary to complete a background check, details on performance decisions and outcomes, performance feedback and warnings, e-learning/training programs, internal and external certifications and membership of professional associations, performance and development reviews (including information you provide when asking for/providing feedback, creating priorities, updating your input in relevant tools, comments from/re. counsellors/counselees), willingness to relocate, driver's license and car ownership information, assessment information and information used to populate employee biographies. **Management records -** Details of any shares of common stock or directorships, stock purchase plans, stock purchase

	eligibility and contribution, stock options information. Website, tools, systems, apps - Information required to access Accenture systems, tools and applications such as System ID, LAN ID, e-mail account, instant messaging account, mainframe ID, previous employee ID, previous manager employee ID, system passwords, access logs, access rights, security level, activity logs, office Wi-Fi connection logs, office access credential data, employee status reason, branch state, country code, previous company details, aggregated/hashed professional email/calendar/IM meta-data, previous branch details, and previous department details, and electronic content produced using Accenture systems, iinformation derived from the deployment and use of information systems and tools including from third parties; tracking data including data from cookies and other technology, visitor logs, IP addresses, individual posts into chat rooms, blogs, circles, comments, systems' recordings such as web meetings, calls and webinars. **Sensitive data -** Certain types of sensitive information when permitted by local law, such as health/medical information (including data required to mitigate health and safety risks – including during a health crisis), trade union membership information, religion, and race or ethnicity, information on criminal convictions and offences. Accenture collects this information for specific purposes, such as health/medical information in order to accommodate a disability or illness and to provide benefits; to get access to and/or to use certain tools or premises; background checks (where permissible under local laws); religion or church affiliation in countries such as Germany where required for statutory tax deductions; and diversity-related personal data (such as race or ethnicity) in order to comply with legal obligations and internal policies relating to diversity and anti-discrimination. Accenture will only use such sensitive information for the purposes provided by law. **Advertising. marketing and public relations -** Promoting and providing products and services to actual and potential customers; advertising, marketing and PR related activities; communications; compliance; business operations; research, complaints and enquiries handling; management of business relationships and other activities; other services.

	Accounts and records data, data relating to vendors, service providers, suppliers, payees and intermediaries, legal services data - Order management, including billing, credit analysis, shipping, account maintenance, and internal administration and accounting for all commercial relationships; managing and analyzing sales and demand; communications; business operations; customer relationship management (e.g., CRM); conducting internal audits and other internal control activities relating to contract; management with customers, suppliers, vendors, subcontractors and business partners; compliance; due diligence for anticorruption and anti-bribery purposes; reporting activities to fulfil finance and accounts requirements; risk management and corporate audits and assessments (e.g., Background Investigations Tool and Gift & Entertainment Hub) Internal investigations (e.g., Business Ethics Helpline); internal investigations; legal filing and reporting; purchase order and payment; computer system security, including ensuring adequate level of protection of the personal data stored therein; other services on an ad-hoc basis. **Data relating to mergers, ventures and acquisitions -** Management and employment information, compensation and payroll data, business operations, customer relationship management, compliance; due diligence, reporting activities to fulfil finance and accounts requirements; risk management and corporate audits and assessments; legal filing and reporting; computer system security, including ensuring adequate level of protection of the personal data stored therein. More information about **categories of personal data** and **purpose of processing** can be found in ANNEX 2 of EU BCR-C : Binding Corporate Rules (BCR) | Accenture **Types of Processing Covered** For the purposes of the UK BCR-C, “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-C 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-C: 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** 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-C") 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-C and are **in addition to** the statutory rights available under the UK data protection framework. Data subjects can then enforce the UK BCR-C against any relevant Participating Entity for breaches it has caused of the UK BCR-C. The Lead UK BCR Member agrees to be fully liable to Relevant Data Subjects and to the ICO 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. These rights allow individuals to enforce compliance with the UK BCR-C, including in relation to: • Data protection principles, lawfulness of processing, security and personal data breach notifications, restrictions on onward transfers • Rights of information, access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, right to protections around automated decision-making under Article 22, right to complain to the controller under

	S164A DPA 2018, right to judicial remedies (including to complain to ICO and/or courts), right to obtain redress and compensation for breaches of UK BCRs. • Jurisdiction and liability provisions; • Transparency and easy access to the UK BCR Summary; • Right to complain through Accenture's internal complaints process; • Cooperation duties with the Commissioner (which also includes obligations related to Art. 47(2)(j) and (k) UK GDPR) relating to compliance obligations covered by the third-party beneficiary clause; • Obligations in case of local laws and practices affecting compliance with the UK BCR and in case of government access requests • And the enforceability of the third-party beneficiary section itself.