Name of the group
Processing activities included into the BCR

Date of update

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

Processing activity	Purposes of the processing	Categories of data subjects	Categories of personal data	Categories of recipients data disclosed to	International Transfer Destination	Place of storage	Time limits for ensure	Technical and organisational security measures applied	Comments
Clients, suppliers and contact person management	maintaining the contractual relationship..	suppliers, clients, contact persons	name, ID number, address, telephone...	Purchasing department, Sales department, Finance department	Morocco...	manual records : - electronic records : -	-	-	If any SAMPLE
Personal details (employment contract) Personal details (clients & prospects) Personal details (vendors, service providers, suppliers, payees and intermediaries, legal services data) Other individuals (alumni, corporate citizenship/outreach, website visitors) Documentation required under immigration laws Compensation and payroll Leaves of absence Pension records Position and contractual information Work location & relocation Talent management information Management records Website, tools, systems, apps Sensitive data Advertising, marketing and public relations Accounts and records data, data relating to vendors, service providers, suppliers, payees and intermediaries, legal services data Data relating to mergers, ventures and acquisitions	Scheduling	Accenture employees (past and present) - includes permanent and contracting staff (temporary or casual workers, freelancers, contractors, trainees).	Personal details [employment contract] - 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 cleaning, damage events, insurance), 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 administration and accounting; curriculum vitae; time and expense records concerning the provision of services; operational data; details of relationship with Accenture.	Accenture entities - Accenture entities which are signed up to the BCR or other Accenture entities/affiliates outside the BCR [using a different transfer mechanism].	Many of our global systems are operated from the US, we also have significant operations in India, Philippines, and China. However, as a global group we transfer to many countries worldwide, inside and outside the EEA, Switzerland, and the UK. We publish a list of Participating Entities that have signed the BCR Intercompany Agreements which is available here.	Manual records: physical registries Electronic records: Cloud storage servers, local secured systems	Policy 1413 – Corporate Records and Information Management defines Accenture's records retention criteria for specific functions and/or legal, regulatory, and business requirements.	The following terms describe the technical and organizational measures, internal controls and information security routines that Accenture maintains to safeguard Personal Data. Accenture may change these measures from time to time, without notice, so long as any such revisions do not materially reduce or degrade the protection provided for the Personal Data. STANDARD DATA SAFEGUARDS: 1.Organization of Information Security Security Ownership. Accenture will appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures. Security Roles and Responsibilities. Accenture's personnel with access to Personal Data will be subject to confidentiality obligations. Risk Management Program. Accenture will have a risk management program in place to identify, assess and take appropriate actions with respect to risks related to the processing of the Personal Data in connection with the applicable agreement between the Parties. 2.Asset Management a.Asset Inventory. Accenture will maintain an asset inventory of its infrastructure, network, applications and cloud environments. Accenture will also maintain an inventory of its media on which Personal Data is stored. Access to the inventories of such media will be restricted to personnel authorized in writing to have such access. b.Data Handling. Accenture will: Classify Personal Data to help identify such data and to allow for access to it to be appropriately restricted. Limit printing of Personal Data from its systems to what is minimally necessary to perform services and have procedures for disposing of printed materials that contain Personal Data.
	Talent Acquisition / Recruitment	Non-employee workers including volunteers, assignees, advisors, consultants, agents and other professional experts, secondees, apprentices, interns, alumni, other third parties.	Individuals identified by the aforementioned data subjects as dependents and beneficiaries, including insured spouses and partners, children, guardians and parents, family members and contact persons for emergencies. Job applicants, candidates and pre-hires.					Require its personnel to obtain appropriate authorization prior to storing Personal Data outside of contractually approved locations and systems, remotely accessing Personal Data, or processing Personal Data outside the Parties' facilities.	
	Management and administration of employees		Client contacts, current and past contacts and prospects – including employees, officers, agents, consultants and other professional experts. Vendor, supplier contacts.					4.Human Resources Security Security Training. Accenture will: Inform its personnel about relevant security procedures and their respective roles. Inform its personnel of possible consequences of breaching the security rules and procedures.	
	Facilitating communication (including in case of emergencies)							Only use anonymous data in its training environments.	
	Operating and managing Accenture's business operations			Professional advisors - Accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors in all of the countries in which Accenture operates.				5.Physical and Environmental Security a.Physical Access to Facilities. Accenture will implement and maintain procedures to limit authorized access to its facilities where information systems that process Personal Data are located.	
	Employee engagement, performance management and professional development			Service providers – Companies that provide products and services to Accenture such as payroll, pension scheme, benefits providers, human resources services, performance, training, expense management, IT systems suppliers and support, advertising and marketing, security and performance monitoring, third parties				b.Physical Access to Equipment. Accenture will maintain records of the incoming and outgoing media containing Personal Data, including the kind of media, the authorized sender/recipients, date and time, the number of media, and the types of Personal Data they contain.	
	Financial planning, payroll, fund management and accounting	Members of the press and other organizations (including charities, educational institutions, Regulators, business intermediaries, etc.).		Public and governmental authorities - Entities that regulate or have jurisdiction over Accenture such as regulatory authorities, law enforcement, public bodies, and judicial bodies.				c.Component Disposal. Accenture will use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) processes to delete Personal Data when it is no longer needed.	
	Share plan management and operations	Website users and complainants, correspondents and enquirers.		Corporate / commercial transaction - A third party in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of Accenture business, assets, or stock (including in connection with any bankruptcy or similar proceedings). A third party in connection with any proposed or actual client project.				5.Communications and Operations Management a.Operational Policy. Accenture will maintain security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Personal Data.	
	Business and market development	Individuals attending our events.						b.Mobile Device Management (MDM)/Mobile Application Management (MAM). Accenture will maintain a policy for its mobile devices that: •Enforces device encryption. •Prohibit use of blacklisted apps. •Prohibits enrollment of mobile devices that have been "jail broken."	
	Advertising, marketing and public relations	Shareholders.	Documentation required under immigration laws - Citizenship, passport data, professional work visa, details of residency or work permit (a physical copy and/or an electronic copy). Compensation and payroll - Remuneration details (including history, base pay and bonus or incentive pay, salary banding, frequency of payments), pay deductions, tax codes, insurance codes and statutory and voluntary contributions, benefits, loans, overtime and shift work, compensation type, pay frequency, salary reviews and performance appraisals, banking details including credit card details (both company and personal where the employee has used this), working time records (including vacation and other absence records, leave status, hours worked and department standard hours), pay data and termination date, compensation details, offers, reductions/reimbursements, employee/capital-forming investments, expense descriptions, amounts claimed and type, approve and pre-approvals, data required to support expenses claims including bills, receipts, documents, interests in businesses and equity holdings.	Clients and prospects – If needed, sharing relevant information about employees/contractors with clients and prospects (including CV information, name and corporate email if required to access client premises/ and other relevant information which would be necessary to share with clients/prospects, subject to applicable laws.				c.Data Recovery Procedures. Accenture will: Have specific data recovery procedures with respect to its systems in place designed to enable the recovery of Personal Data being maintained in its systems. Review its data recovery procedures at least annually. Log data recoverative efforts with respect to its systems, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.	
	Building and managing external relationships	Alumni.		Corporate citizenship - Corporate citizenship partners/organizations where necessary (e.g., to obtain documentation related a gift or a tax statement).				d.Malicious Software. Accenture will have anti-malware controls to help avoid malicious software gaining unauthorized access to Personal Data, including malicious software originating from public networks.	
	Maintaining relationships with former employees and alumni relations	Children and adolescents via our Corporate Citizenship, intern and outreach programs.						e.Data Beyond Boundaries. Accenture will: Encrypt Personal Data that it transmits over public networks.	
	Planning and delivery of business integration capabilities	Other third parties.						Protect Personal Data in media leaving its facilities (e.g., through encryption).	
	Research and development		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 review (including start date, end date, temporary suspension), illness including accidents at work and occupational health (in accordance with local law). Dates (beginning, and end duration).						Implement automated tools where practicable to reduce the risks of misdirected email, letters, and / or faxes from its systems.	
	Compliance, audit and insurance purposes, including supplier and customer due diligence		Pension records - Monthly pension, yearly pension, capital sums, deferred compensation sums, type of pension plan; other data related to pension fund (including enrollment and discharges, contribution data and insurance period in the statutory Social Security).					f.Event Logging For its systems containing Personal Data, Accenture will log events consistent with its stated policies or standards.	
	Internal and external investigations including liaison with law enforcement/other government agencies where required to do so by law							6.Access Control a.Access Policy. Accenture will maintain a record of security privileges of individuals having access to Personal Data via its systems.	
	Litigation management							b.Access Authorization. Accenture will:	
	Client, supplier and business intermediary/partner management		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 managerial 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 specializations 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. counsellor/counsellees), willingness to relocate, driver's license and car ownership information, assessment information and information used to populate employee biographies.						Maintain access controls and policies to manage what access is allowed to the systems with respect to Personal Data on a minimum necessary basis. Such controls and policies will include: •Review of key personnel's rights at least every six months. •Immediately revoking access to all systems and resources after termination of an employee or other person's relationship with Accenture. •Promptly revoking or changing rights in response to changes in jobs. •Restricting access to Personal Data in its systems to only those individuals who require such access to perform their job function. •Limit access to Personal Data in its systems to only that data minimally necessary to perform the services. •Support segregation of duties between its environments so that no individual person has access to perform tasks that create a security conflict of interest (e.g., developer/ reviewer, developer/tester). d.Integrity and Confidentiality. Accenture will instruct its personnel to disable administrative sessions when leaving premises or when computers are otherwise left unattended.	
	Travel management							e.Authentication. Accenture will: Use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) practices to identify and authenticate users who attempt to access its information systems.	
	Knowledge management							•Where authentication mechanisms are based on passwords, require that the passwords are renewed regularly.	
	Corporate Citizenship and outreach programs							•Where authentication mechanisms are based on passwords, require the password to contain at least eight characters and three of the following four types of characters: numeric (0-9), lowercase (a-z), uppercase (A-Z), special (e.g., !, *, &, etc.).	
	Complying with legal requirements							•Ensure that deactivated or expired identifiers are not granted to other individuals.	
	Reporting to data privacy supervisory authorities - routine reporting and breach notification							•Monitor repeated attempts to gain access to its information systems using an invalid password.	
	Liaising with regulatory/government departments for routine reporting requirements under law – tax, social security, benefits, national ID programs							Maintain industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) procedures to deactivate passwords that have been corrupted or inadvertently disclosed.	
	Mergers & Acquisitions – this includes due diligence and information relevant to potential ventures, joint ventures, mergers and acquisitions							Use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, as well as during storage.	
	Social listening – identifying and assessing what is being said about Accenture and our clients on social media (only publicly accessible content)							f.Multi Factor Authentication. Accenture will implement Multi-Factor Authentication for internal access and remote access over virtual private network (VPN) to its systems.	
	Incentives data analytics, including analysis of our applicant pool in order to better understand who is applying to positions at Accenture and how to attract and keep top talent							7.Penetration Testing and Vulnerability Scanning of Accenture Systems. a.At least annually, Accenture will perform penetration and vulnerability assessments on Accenture's IT environments in accordance with Accenture's internal security policies and standard practices.	
	Other purposes not incompatible with the ones listed above or other purposes required and/or permitted by law or regulation							b.Accenture agrees to share with Client summary level information related to such tests as conducted by Accenture to the extent applicable to the Services.	
								c.For clarity, as it relates to such penetration and vulnerability testing, Client will not be entitled to (i) data or information of other customers or clients of Accenture; (ii) test third party IT environments except to the extent Accenture has the right to allow such testing; (iii) any access to or testing of shared service infrastructure or environments; or (iv) any other Confidential Information of Accenture that is not directly relevant to such tests and the Services.	
								d.For any Accenture IT systems that are physically dedicated to Client, the Parties may agree to separate, written testing plans and such testing will not to exceed two tests per year.	
								8.Network and Application Policy and Hardening. Accenture will	