Name of the group		Date of update								
Processing activities included into the BCR										
This table sets out the types of individuals we generally process Personal Data about, the categories of Personal Data, and the purposes for which we process Personal Data about them when we operate as a Data Processor on behalf of our Clients. The information provided is a generic summary. It does NOT mean we process all these data Personal Data categories about all the types of individuals. Each Client Service Agreement stipulates the relevant categories of individuals, processing and purposes specific to that particular Client engagement.										
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 erasure**	**Technical and organisational security measures applied**	**Comments**
clients, suppliers and contact person management	maintaining the contractual relationship…	suppliers, clients, contact persons	name, ID number, adress, telephone…	Purchasing department, Sales departement, Finance departement	Morocco…	manual records : … ; electronic records : …	…	…	if any
Access Control & Credentials Data Accounts Payable & Receivable Processing Advertising Application Development, Maintenance, Support and Testing Application Training and/or User Support Artificial Intelligence (AI) Billing and Payment Processing Blockchain Credit and Collections Call Centre Cloud Consulting and/or Data Analysis Content Creation Content Moderation Creation of Communications Data Conversion Financial Crime Prevention Hosting Services HR and Payroll Services Industry X Marketing Market research Procurement Profiling and aggregation Quantum Computing Security Services Social Media Listening	Access Control & Credentials Data – Personal Data processed for the purposes of identifying authorised users of any cloud and other services, platforms, websites etc., and for the purposes of identifying the access/authority level such users have been granted.	Client employees (past and present) – includes permanent and contracting staff (temporary or casual workers, freelancers, contractors, trainees)	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, family situation. This could also include data that could be indicative of personal habits or interests like browsing data, purchasing data, social medial 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 behaviour 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 behaviour of use Consumer Profiles Including Marketing Profiles – profiles of consumer or individual preferences and behaviour 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 behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images, iris scans, finger prints 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 – There may be other types of Personal Data not specified here but unique to client processing of Personal Data.	Accenture operates in a highly networked environment where numerous entities are involved in the development, design, production, delivery and maintenance lifecycle and can therefore be involved as data importers and exporters. Accenture entities – Accenture entities which are signed up to the Processor BCR or other Accenture entities/affiliates outside the Processor BCR (using a different transfer mechanism where required) and whether they act as data exporters or importers. Client entities – where there are direct transfers from Clients to non-EEA Accenture Participating Entities. Professional advisors – Accountants, auditors, lawyers, insurers and other outside professional advisors. Service providers – For any of the purposes or processing mentioned above, we may use companies that support Accenture's client delivery services by providing products and services as part of our Client offerings such as accounts payable and receivable, billing, payroll, pension scheme, benefits providers, human resources services, performance, training, expense management, IT systems suppliers and support including application development, testing services, hosting service providers, cloud partners, credit card companies, medical or health practitioners, trade bodies and associations, and other service providers. Public and governmental authorities – Entities that regulate or have jurisdiction over Accenture such as regulatory authorities, law enforcement, public bodies, and judicial bodies.	Cross Border Transfers can occur to any country, as the aforementioned entities may be located worldwide. This applies not just to Accenture as a global group but also global Clients and suppliers globally. 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. We publish a list of group companies that have signed the Processor BCR Intercompany Agreements which is available here. Insert link Our Sub processors are located worldwide. Clients are provided with specific information about relevant Sub processors, including their locations in accordance with applicable laws and as per relevant service agreements which reflect their Individual Rights.	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. 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. 3.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. Only use anonymous data in its training environments. 4.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. b.Physical Access to Components. 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. 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. 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. 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." 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 restoration 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. 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. e.Data Beyond Boundaries. Accenture will: Encrypt Personal Data that it transmits over public networks. Protect Personal Data in media leaving its facilities (e.g., through encryption). Implement automated tools where practicable to reduce the risks of misdirected email, letters, and / or faxes from its systems. f.Event Logging. For its systems containing Personal Data, Accenture will log events consistent with its stated policies or standards. 6.Access Control a.Access Policy. Accenture will maintain a record of security privileges of individuals having access to Personal Data via its systems. b.Access Authorization. Accenture will: -Maintain and update a record of personnel authorized to access Personal Data via its systems. -When responsible for access provisioning, promptly provision authentication credentials. -Deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed 90 days). -Deactivate authentication credentials upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.) within two business days. -Identify those personnel who may grant, alter or cancel authorized access to data and resources. -Ensure that where more than one individual has access to its systems containing Personal Data, the individuals have unique identifiers/log-ins (i.e., no shared ids). c.Least Privilege. Accenture will: -Only permit its technical support personnel to have access to Personal Data when needed -Maintain controls that enable emergency access to productions systems via firefighter ids, temporary ids or ids managed by a Privileged Access Management (PAM) solution. -Restrict 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. 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. -Where authentication mechanisms are based on passwords, require that the passwords are renewed regularly. -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.). -Ensure that de-activated or expired identifiers are not granted to other individuals. -Monitor repeated attempts to gain access to its information systems using an invalid password. -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. -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. f.Multi Factor Authentication. Accenture will implement Multi-Factor Authentication for internal access and remote access over virtual private network (VPN) to its systems. 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. 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 Design and Management. Accenture will: •Have controls to avoid individuals gaining unauthorized access to Personal Data in its systems. •Use email-based data loss prevention to monitor or restrict movement of sensitive data. •Use network-based web filtering to prevent access to unauthorized sites. •Use firefighter IDs or temporary user IDs for production access. •Use network intrusion detection and / or prevention in its systems. •Use secure coding standards. •Scan for and remediate OWASP vulnerabilities in its systems. •To the extent technically possible, expect that the Parties will work together to limit the ability of Accenture personnel to access non-Client and non-Accenture environments from the Client systems. •Maintain up to date server, network, infrastructure, application and cloud security configuration standards. •Scan its environments to ensure identified configuration vulnerabilities have been remediated. 9.Patch Management. Accenture will have a patch management procedure that deploys security patches for its systems used to process Personal Data that includes: Defined time allowed to implement patches (not to exceed 90 days for high or medium patches as defined by Accenture's standard); and Established process to handle emergency or critical patches as soon as practicable. 10.Workstations. Accenture will implement controls for workstations it provides that are used in connection with service	
	Accounts Payable & Receivable Processing – we provide account payable and accounts receivable services for Clients – this includes processing information provided by Clients about payments and transactions such as bank account information.	Client non-employee workers including volunteers, assignees, secondees, apprentices, interns							
	Advertising – we provide advertising and brand services for Clients, including the ability to track the success and uptake of advertising by users and to analyse the targeting and effectiveness of advertising campaigns.	Individuals identified by the aforementioned data subjects as dependents and beneficiaries, including spouses and partners, children, guardians and parents, family members and contact persons for emergencies							
	Application Development, Maintenance, Support and Testing – we provide application services to Clients – this may include product design and development, maintenance services, technical support services, application enhancements and integration, implementation, configuration, customization and testing.	Client job applicants, candidates and pre-hires							
	Application Training and/or User Support – we provide training and user support where we have access to a Client training environment and or/provide user support for Client systems.	Client contacts, current and past contacts and prospects - including employees, officers, agents, consultants and other professional experts							
	Artificial Intelligence (AI) – we provide services for Clients using artificial intelligence technology and we use data to train AI algorithms for this purpose.	Client actual and potential customers, end-users and consumers							
	Billing and Payment Processing – we provide billing and payment management and support services for Clients using billing and payment information provided by the Client relating to their customers, partners and/or suppliers.	Client vendor, supplier contacts, including their permanent and contracting staff							
	Blockchain – we provide services using an open, distributed ledger technology which records transactions and other information shared between multiple parties.	Members of the press and other organizations (including charities, educational institutions, regulators, business intermediaries, etc.)							
	Credit and Collections – we provide credit and collection services on behalf of Clients using information provided by the Client which may include credit information and collection history about their customers.	Client website users and complainants, correspondents and enquirers							
	Call Centre – we provide call-centre based services for Clients with access to their systems and customers' information.	Individuals attending client events, whether in person or virtual participation which we organise on behalf of clients							
	Cloud – we provide and/or implement cloud solutions and platforms for systems containing Client data. We also commercialize proprietary or third-party software products that ingest Client data.	Client shareholders							
	Consulting and/or Data Analysis – we provide consulting and data analysis services to Clients which may include preparing and developing reports analysing client data including data belonging to its employees and customers, and data from other third parties.	Client alumni							
	Content Creation – we provide content services where we may produce text, digital content, film, photo, audio, graphics or other types of content for Clients.	Children and adolescents' information where relevant to a client organisation							
	Content Moderation – we provide content moderation services to Clients.	Client business partner and joint venture contacts - their employees, contractors, suppliers, customers or other third parties							
	Creation of Communications – we provide content services which may include producing newsletters, print communications, advertising and marketing material.	Client ventures and acquisitions target company contacts, employees, contractors, suppliers, customers or other third parties							
	Data Conversion – we provide data conversion services, for example, transitioning data from one format and source to a different format and destination, for example moving data from an old system to a new system or different platform.	Other third parties to whom personal data provided by Clients to Accenture belongs							
	Financial Crime Prevention – we provide integrated Anti Money Laundering Services for KYC (Know Your Customer), Transaction Monitoring and Sanctions based on a 'run-as-a-service' model. This also includes Client lifecycle management and model validation.								
	Extended/Virtual Reality – we provide services using technology to create a simulated environment, such as virtual reality and augmented reality.								
	Hosting Services – we provide services to (i) manage Client systems hosted by Accenture, (ii) manage systems hosted in a Client environment or (iii) be responsible for overseeing and managing third parties hosting Client data.								
	HR and Payroll Services – we provide HR and payroll management services to Clients. This means we have access to Client systems and their employee information including Sensitive Personal Data, where applicable and financial Personal Data such as salary information.								
	Industry X – we provide services to help our Clients design, manufacture and design next generation products and factories. Services include without limitation using Client product or manufacturing related data to create "digital twins" to track product lifecycles from design through repair and services that use various IoT sensors that collect and track data.								
	Marketing – we provide marketing services to Clients, including analytics of market segments, personalization of marketing, and delivery of marketing communications to individuals on behalf of Client via a variety of means including e-mail, SMS, social media, search and web.								
	Market research – we carry out market research, asking individuals questions and gathering data and feedback from individuals, to refine and deliver services to Clients.								
	Procurement – we manage procurement processes on behalf of Clients including having access to quotations, client specific pricing information, specific client requirements, specification of the requirements and other procurement related info.								
	Profiling and aggregation – we provide marketing and data analytics services to create aggregated reports and statistics and also to create and use profiles of individuals, including their characteristics, behaviours and preferences using the data that has been provided for the other purposes listed								
	Quantum Computing – we develop processes that utilize Quantum bits.								
	Security Services, including managed security services – we provide a range of services to enable Clients to plan for, defend against and respond to cyberattacks and build their cyber resilience - including providing security strategy, risk and compliance consulting, assessing clients security posture, services designed to help Clients prevent and defend against attacks (from application scanning and penetration testing to advanced adversary services and threat hunting as well as monitoring and detection response services) and respond to attacks (forensic investigation and incident response), assisting Clients with identity and access management and operating clients' security operations functions. Security services also include cyber threat intelligence services, that might entail searching for client leaked information and personal data in the web.								
	Social Media Listening – we provide services to Clients to monitor and analyse what people are saying about a Client or competitor on social media, collect and analyse such data and use it to provide report and recommendations to Clients.								
	Staging and Migration Services – we provide a range of staging and migration services which include maintenance of staging environments, migration services including roll out preparation, archiving or decommissioning of applications, system implementation and upgrades where we will have access to client data.								
	Technical Support - includes provision of technical IT support to clients, including technical support on Accenture-provided tools/platforms used to deliver services to clients								
	User Acceptance Testing – we provide services where we perform UAT with access to a client network/domain or via Accenture's network. As part of performing these services, we may have access to client data.								
	User Data – we capture data concerning user patterns, consumption, behaviour across various cloud and other services, platforms, applications, apps, websites etc. for the purposes of analysing such users' data and for improving the user interface and performance of such services etc.								

	Further Purposes and Processing – we may be asked to provide services unique to a specific client requirement.							delivery/receipt incorporating the following: •Software agent that manages overall compliance of workstation and reports at a minimum on a weekly basis to a central server •Encrypted hard drive •Patching process so that workstations are patched within the documented patching schedule •Ability to prevent blacklisted software from being installed •Antivirus with a minimum weekly scan •Firewalls installed 11.Information Security Breach Management. a.Security Breach Response Process. Accenture will maintain a record of its own security breaches in its systems with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the process for recovering data. b.Service Monitoring. Accenture's security personnel will review their own logs as part of their security breach response process to propose remediation efforts if necessary. 12.Business Continuity Management. Accenture will have processes and programs that are aligned to ISO 22301 to enable recovery from events that impact its ability to perform in accordance with the Agreement. SUPPLEMENTARY MEASURES. In addition, in accordance with regulatory guidance following the European Court of Justice "Schrems II" decision, Accenture further commits to maintaining the following additional technical, organizational and legal/contractual measures with respect to personal data. Technical Supplementary Measures: The Personal Data in transit between Accenture entities will be strongly encrypted with encryption that: •Is state of the art, •Secures the confidentiality for the required time period, •Is implemented by properly maintained software, •Is robust and provides protection against active and passive attacks by public authorities, including crypto analysis, and •Does not contain back doors in hardware or software, unless otherwise agreed with the applicable Personal. The Personal Data at rest and stored by any Accenture entities will be strongly encrypted with encryption that: •Is state of the art, •Secures the confidentiality for the required time period, •Is implemented by properly maintained software,	