ACCENTURE

GLOBAL DATA PRIVACY STATEMENT

Effective date: September 2018

We may modify, add or remove portions of our Global Data Privacy Statement from time to time. If we decide to change our Global Data Privacy Statement, we will post the updated Global Data Privacy Statement on our internal Accenture portal. From the first day of employment, you can log in to our internal Accenture portal, where you will be shown the most recent version of our Global Data Privacy Statement.

1. GENERAL INFORMATION

PRIVACY STATEMENT This global privacy statement explains how Accenture PLC and/or its affiliates ("Accenture") protect the personal data Accenture processes and controls relating to you ("your personal data"), why Accenture processes your personal data, who has access to your personal data and how you can exercise your rights in relation to the processing of your personal data.

Further information on Accenture (and, if relevant, its representative) can be found **here**. Any Accenture entity located outside the European Union will for the purposes of compliance with data privacy laws be represented by Accenture PLC.

This global privacy statement provides an overview of Accenture's most common processing activities of your personal data. Please note that certain specific processing activities may be subject to a separate and tailored privacy statement.

In the event any translation of this global privacy statement is prepared, the English version of this global privacy statement shall prevail in case of conflicts between the different language versions.

Which categories of personal data does Accenture process?

Accenture will collect personal data about you to achieve the purposes set out in this global privacy statement.

For further information on the specific categories of personal data Accenture is processing, please see **section 2**. For further information on the sources from which Accenture has obtained your personal data, please see **section 3**.

If you provide Accenture with any personal data of another person (for instance, a potential employee/referral), you are responsible for ensuring that such person is made aware of the information contained in this global privacy statement and that the person has given you his/her consent for sharing the information with Accenture.

Except for certain information that is required by law, your decision to provide any personal data to Accenture is voluntary. You will therefore not be subject to adverse consequences if you do not wish to provide Accenture with your personal data. However, please note that if you do not provide certain information, Accenture may not be able to accomplish some or all of the purposes outlined in this global privacy statement, and you may not be able to use certain tools and systems which require the use of such personal data.

Why does Accenture process your personal data?

Accenture may collect, use, transfer, disclose and otherwise process your personal data in the context of managing Accenture's contractual and/or employment relationship with you, facilitating communication with you (including in case of emergencies), operating and managing Accenture's business operations, complying with legal requirements, monitoring your use of Accenture's systems and undertaking data analytics. For a more detailed list of the purposes, please see **section 4**.

Accenture will not use your personal data for purposes that are incompatible with the purposes listed in this global privacy statement, unless it is required or authorized by law, or it is in your own vital interest (e.g. in case of a medical emergency) to do so.

On which legal basis does Accenture process your personal data?

Accenture processes your personal data as permitted by applicable data privacy laws and its internal policies, including Accenture's Global Data Privacy Policy 0090.

Accenture processes your personal data for the purposes set out in this global privacy statement for one or more of the following reasons: (i) because Accenture is required to do so for compliance with a legal obligation to which it is subject, (ii) because such information is necessary for the performance of a contract to which you are a party, (iii) because the processing is necessary for the purposes of the legitimate interests pursued by Accenture or by a third party (as described in the last sentence of this paragraph), or (iv) where necessary in order to protect the vital interests of any person. Accenture has legitimate interests in collecting and processing personal data, for example: (1) to ensure that Accenture's networks and information are secure, (2) to administer and generally conduct business and (3) to prevent fraud.

In addition, Accenture may process your sensitive data and/or make automated decisions concerning you, where permitted by applicable law and/or with your prior consent.

Please see **section 5** for further information on the legal basis on which Accenture bases the processing of your personal data for each processing activity.

Who has access to your personal data?

Access to your personal data within Accenture will be limited to those employees who have a need to know the information for the purposes described in this global privacy statement, which may include your managers and their designees, as well as personnel in Security, HR, IT, Compliance, Legal, Finance and Accounting, Corporate Investigations and Internal Audit. All employees within Accenture will generally have access to your business contact information (e.g. name, position, telephone number and e-mail address).

Furthermore, your personal data may be transferred to other Accenture offices and third parties, which may involve transferring your personal data to other countries.

As a global organization with offices and operations throughout the world, your personal data may be transferred or be accessible internationally throughout Accenture's global business and between its entities and affiliates. Any transfers of your personal data to other Accenture offices (including transfers from within the European Economic Area (EEA) to outside the EEA) will be governed by Accenture's binding corporate rules (BCR; a copy of which can be found **here**). Accenture's BCR reflect the standards contained in European data privacy laws (including the General Data Protection Regulation). Having the BCR means that all Accenture's group entities which have signed up to the BCR have to comply with the same internal rules. It also means that your rights stay the same no matter where your data are processed by Accenture. A list of the Accenture offices that may process your personal data, and their contact information, can be found **here**.

Furthermore, where there is a need, Accenture may share your personal data with third parties, such as service providers and public authorities. Before doing so, Accenture takes steps to protect your personal data. Any third party service providers and professional advisors to whom your personal data are disclosed, are expected and required to protect the confidentiality and security of your personal data and may only use your personal data in compliance with applicable data privacy laws. For the categories of third parties with which Accenture may share your personal data, please see **section 6**. Unless you are otherwise notified, any transfers of your personal data from within the EEA to third parties outside the EEA will be based on an adequacy decision or are governed by the EU standard contractual clauses (a copy of which can be obtained from dataprivacy@accenture.com). Any other, non-EEA originating, international transfers of your personal data, will take place in accordance with the appropriate international data transfer mechanisms and safeguards.

How does Accenture protect your personal data?

Accenture maintains organizational, physical and technical security arrangements for all the personal data it holds. Accenture has protocols, controls and relevant policies, procedures and guidance to maintain these arrangements taking into account the risks associated with the categories of personal data and the processing Accenture undertakes.

Accenture adopts market leading security measures to protect your personal data. This includes (without being limitative):

- Accenture holds an ISO27001 certification, which indicates that it adheres to the highest and strictest information security standards. This is a security standard awarded by the British Standards Institution that serves as international certification that Accenture adheres to the highest and strictest standards. This certification is the only auditable international standard that defines the requirements for an Information Security Management System, and confirms that Accenture's processes and security controls provide an effective framework for protecting its clients' and its own information.

- Accenture has regular penetration testing performed by a third party provider, which continues to show the strength of its technical defenses.

How long does Accenture retain your personal data?

Accenture retains your personal data only for as long as is necessary. Accenture maintains specific records management and retention policies and procedures, so that personal data are deleted after a reasonable time according to the following retention criteria:

- Accenture retains your personal data as long as it has an ongoing relationship with you.

- Accenture retains your personal data for as long as needed in order to comply with a legal obligation to which it is subject.

- Accenture retains your personal data where this is advisable to safeguard or improve Accenture's legal position (for instance in relation to statutes of limitations, litigation, or regulatory investigations).

For further information on Accenture's retention policy, please see Accenture's Corporate Records and Information Management guidelines outlined in Accenture's Policy 1413.

Please keep your personal data at all times up to date and inform Accenture of any material changes to your personal data.

Which rights do you have concerning your personal data?

Please contact dataprivacy@accenture.com if you (i) have any questions or concerns about how Accenture processes your personal data or (ii) want to exercise any of your rights in relation to your personal data.

You have the right (in the circumstances and under the conditions, and subject to the exceptions, set out in applicable law to:

- Request access to the personal data Accenture processes about you: this right entitles you to know whether Accenture holds personal data of you and, if so, obtain information on and a copy of those personal data.
- Request rectification of your personal data: this right entitles you to have your personal data be corrected if it is inaccurate or incomplete.
- Object to the processing of your personal data: this right entitles you to request that Accenture no longer processes your personal data.
- Request the erasure of your personal data: this right entitles you to request the erasure of your personal data, including where such personal data would no longer be necessary to achieve the purposes.
- Request the restriction of the processing of your personal data: this right entitles you to request that Accenture only processes your personal data in limited circumstances, including with your consent.
- Request portability of your personal data: this right entitles you to receive a copy (in a structured, commonly used and machine-readable format) of personal data that you have provided to Accenture, or request Accenture to transmit such personal data to another data controller

To the extent the processing of your personal data falls in scope of Accenture's BCR, you may also want to review your rights under Accenture's BCR.

To the extent that the processing of your personal data is based on your consent, you have the right to withdraw such consent at any time by contacting Accenture's data protection officer at dataprivacyofficer@accenture.com. Please note that this will not affect Accenture's right to process personal data obtained prior to the withdrawal of your consent, or its right to continue parts of the processing based on other legal bases than your consent.

Please note, however, that certain personal data may be exempt from the above-mentioned rights pursuant to applicable data privacy or other laws and regulations.

If, despite Accenture's commitment and efforts to protect your personal data, you believe that your data privacy rights have been violated, Accenture encourages and welcomes you to come to Accenture first to seek resolution of any complaint. You have the right at all times to register a complaint directly with the relevant supervisory authority or to make a claim against Accenture with a competent court (either in the country where you live, the country where you work or the country where you deem that data privacy law has been infringed).

What if you have questions or want further information?

This global privacy statement, and the web pages referred to therein, aims to give you complete and transparent information on how Accenture processes your personal data.

If you have any further questions or concerns regarding how Accenture processes your personal data, or if you wish to exercise any of your foregoing rights, please contact dataprivacy@accenture.com.

You also may contact the Data Protection Officer at dataprivacyofficer@accenture.com.

2. FURTHER INFORMATION ON CATEGORIES OF PERSONAL DATA

The below table sets out the categories of personal data that Accenture processes in the context of the processing activities described in the global privacy statement.

Category of personal data	Explanation
Personal details.	Name, preferred pronoun, all types of contact details (such as e-mail, phone numbers, physical address), gender, date of birth, age, place of birth, national identification number, social security and health insurance number, insurance information, marital/civil partnership status, domestic partners, dependents, emergency contact information, military history.
Sensitive data.	Accenture may collect certain types of sensitive information when permitted by local law or with your consent, such as health/medical information (including disability status), trade union membership information, religion, race or ethnicity, minority flag, and (where authorized by law) 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; background checks; 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 described in **section 4**
Audiovisual materials.	Photograph, and images/footage captured on CCTV or other video systems, voice recordings.
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 base pay and bonus or incentive pay), benefits, overtime and shift work, compensation type, pay frequency, salary reviews and performance appraisals, banking details, tax details, 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, pension details, interests in businesses and equity holdings.
Position and contractual information.	Description of current position, job title, terms and conditions of employment, membership of the board of directors, information on extent of shareholding, corporate status, career level, management category, job code, job function(s), legal employer entity, location, Accenture contact(s), employee identification number, terms of employment or contract, work history, hire/re-hire and termination date(s) and reason, information from exit interviews/termination documents, length of service, retirement eligibility, promotions and disciplinary records, date of transfers, and reporting manager(s) information.

Talent management information.	Details contained in letters of application and resume/CV or other provided documents (previous employment background, education history, professional qualifications, language and other relevant skills, certification, certification expiration dates), information of recruitment interviews/check lists, information necessary to complete a background check, details on performance decisions and outcomes, performance feedback and warnings, e-learning/training programs, performance and development reviews (including information you provide when asking for/providing feedback, creating priorities, updating your input in relevant tools, comments from/re. counselors/counselees), willingness to relocate, driver's license and car ownership information, and information used to populate employee biographies.
Management records.	Details of any shares of common stock or directorships.
System and application access data.	Information required to access Accenture systems 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, activity logs, employee status reason, branch state, country code, previous company details, previous branch details, and previous department details, and electronic content produced using Accenture systems.

3. FURTHER INFORMATION ON SOURCES OF PERSONAL DATA

Your personal data have been obtained by Accenture from the sources set out in the below table.

Source from which Accenture obtains the personal data
Employees, contractors, (prospective) members of board of directors and shareholders.
Accenture's affiliates.
Employers of the individual contractors.
Public authorities.
Public websites and social media.
Previous employers.
Educational institutions.
Suppliers and vendors.
Background check providers.
Talent management providers.

The above sources are private sources, unless where the source is expressly stated to be "public". Note that these sources may have been holding your personal data both inside and outside the EU.

4. FURTHER INFORMATION ON THE PURPOSES

As set out in the global privacy statement, Accenture processes your personal data for multiple purposes. The below table sets out each of the purposes for which Accenture processes your personal data.

Purpose	Explanation
Managing Accenture's contractual and/or employment relationship with you.	Managing work activities and personnel generally, including management and administration of personnel, recruitment, appraisals, performance, roll-on, roll-off from client projects, promotions and succession planning, rehiring, financial planning, administering salary, and payment administration and reviews, wages and other awards such as stock options, stock grants and bonuses, healthcare including mandatory medical examinations where applicable, pensions and savings plans, training, leave, managing sickness leave, promotions, transfers, secondments, management of inclusion and diversity program, honoring other contractual benefits, organizing recreational activities, organizing corporate citizenship activities (such as employee volunteering), providing employment references, loans, performing workforce analysis and planning, performing employee surveys, performing background checks, managing coaching, disciplinary matters, grievances and terminations, reviewing employment decisions, making business travel arrangements, managing business expenses and reimbursements, planning and monitoring of training requirements and workforce planning, talent management including scheduling, staffing, resource allocation, reporting, career development activities and managing skills and learning path, and creating and maintaining one or more internal employee directories.
Facilitating communication with you (including in case of emergencies).	Facilitating communication with you, ensuring business continuity, providing references and recommendations, protecting the health and safety of employees and others, safeguarding IT infrastructure, office equipment and other property, facilitating communication with you and your nominated contacts in an emergency, facilitating communications to the board of directors of board meeting materials and confidential information.
Operating and managing Accenture's business operations.	Operating and managing the IT and communications systems, including provision and support of network, data, telecom and other IT infrastructure, application hosting, data storage, backup and restore, messaging and collaboration applications, middleware applications, end user services (e.g., desktop and mobile computing and remote access), IT security operations, and related development, support and maintenance services, security access control to facilities, managing product and service development, improving products and services, managing Accenture assets, allocating Accenture assets and human resources, offering services to Accenture's clients/potential clients, strategic planning, project management, business continuity and disaster recovery, compilation of audit trails and other reporting tools, maintaining records relating to business activities, budgeting, financial management and reporting, communications,

	employee service management and internal service request support, managing mergers, acquisitions, sales, re-organizations or disposals, corporate citizenship activities and integration with purchaser, managing risk management and quality operations, organizing and managing the board of directors and shareholder meetings.
Complying with legal requirements.	Complying with legal requirements, such as income tax and national insurance deductions, mandatory filings, record-keeping and reporting obligations, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claims, conducting investigations and complying with internal policies and procedures, protecting, enforcing or defending the legal rights, privacy, safety, or property of Accenture, Accenture affiliates or their employees, agents and contractors (including enforcement of relevant agreements and terms of use), protecting the safety, privacy, and security of users of Accenture products or services or members of the public, or protecting against fraud or for risk management purposes.
Monitoring your use of Accenture's systems.	Monitoring activities as permitted by local law and/or in accordance with Accenture's internal Policy 0057 (including monitoring telephone, e-mail, Internet and other Accenture resources).
Undertaking data analytics	Apply analytics to business operations and data to describe, predict and improve business performance within Accenture and/or to provide a better user experience. Specifically, areas within analytics include descriptive analytics, predictive analytics, analytics involving individuals (clients, employees) use personal data, analytics driven by marketing, single customer view and customer journey, talent/employee management analytics.

Please note that:

- Where the above table states that Accenture relies on its legitimate interests for a given purpose, Accenture is of the opinion that its legitimate interests are not overridden by your interests, rights or freedoms given (i) the transparency Accenture provides on the processing activity, (ii) Accenture's privacy by design approach, (iii) Accenture's regular privacy review and (iv) the rights you have in relation to the processing activity. If you wish to obtain further information on this balancing test approach, please contact dataprivacy@accenture.com.
- Where any of the above purposes require the processing of sensitive data, Accenture will only do so where permitted under applicable law, or with your prior consent.
- Where any of the above purposes involve an automated decision, Accenture will only make such automated decision with your prior consent and after having informed you of meaningful information about the logic involved in the automated decision, as well as the significance and the envisaged consequences of such automated decision for you.
- Accenture will process your personal data based on your prior consent to the extent such consent is required by mandatory law.

5. FURTHER INFORMATION ON LEGAL BASIS

Accenture processes your personal data based on the legal bases set out in the below table.

Purpose	Legal basis
Managing Accenture's contractual and/or employment relationship with you.	Necessary for the performance of a contract to which you are a party.
Facilitating communication with you (including in case of emergencies).	Justified on the basis of Accenture's legitimate interests for ensuring proper communication and emergency handling within the organization.
Operating and managing Accenture's business operations.	Justified on the basis of Accenture's legitimate interests for ensuring the proper functioning of its business operations.
Complying with legal requirements.	Necessary for the compliance with a legal obligation to which Accenture is subject.
Monitoring your use of Accenture's systems.	Justified on the basis of Accenture's legitimate interests of avoiding non-compliance and protecting its reputation.
Undertaking data analytics.	Justified on the basis of Accenture's legitimate interests of analyzing and improving the proper functioning of its business operations.

Please note that:

- where the above table states that Accenture relies on its legitimate interests for a given purpose, Accenture is of the opinion that its legitimate interests are not overridden by your interests, rights or freedoms given (i) the transparency Accenture provides on the processing activity, (ii) Accenture's privacy by design approach, (iii) Accenture's regular privacy review and (iv) the rights you have in relation to the processing activity. If you wish to obtain further information on this balancing test approach, please contact dataprivacy@accenture.com.

- where any of the above purposes require the processing of sensitive data, Accenture will only do so where permitted under applicable law, or with your prior consent.

- where any of the above purposes involve an automated decision, Accenture will only make such automated decision with your prior consent and after having informed you of meaningful information about the logic involved in the automated decision, as well as the significance and the envisaged consequences of such automated decision for you.

- Accenture will process your personal data based on your prior consent to the extent such consent is required by mandatory law.

6. FURTHER INFORMATION ON CATEGORIES OF THIRD PARTY RECIPIENTS

In addition to transferring personal data to its affiliates and relevant internal staff, Accenture may also transfer your personal data to the categories of unaffiliated third parties set out in the below table.

Category of third party	Explanation
Professional advisors.	Accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors in all of the countries in which Accenture operates.
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, third parties assisting with equity compensation programs, 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.
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.