PERSONAL DATA PROTECTION POLICY

1. Purpose, Scope, and Users

PAUL DE MONTGOLFIER ET ASSOCIES LIMITED ("AJC") strives to comply with applicable laws and regulations related to Personal Data protection in countries where AJC operates. This Policy sets forth the basic principles by which AJC processes the personal data of consumers, customers, suppliers, business partners, employees, and other individuals, and indicates the responsibilities of its business departments and employees while processing personal data. The users of this document are all employees, permanent or temporary, and all contractors working on behalf of AJC within the EEA.

2. Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation:

Personal Data
Any information relating to an identified or identifiable natural person ("Data Subject") who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Personal Data
Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller
The natural or legal person, public authority, agency, or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data. Data Processor: A natural or legal person, public authority, agency, or any other body which processes personal data on behalf of a Data Controller.

Processing
An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data. Anonymization: Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

Pseudonymization
The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymization reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymized data is still personal data, the processing of pseudonymized data should comply with the Personal Data Processing principles.

Supervisory Authority
An independent public authority which is established by a Member State pursuant to Article 51 of the EU GDPR.

Lead supervisory authority
The supervisory authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data; it is responsible, among others, for receiving the data breach notifications, to be notified on risky processing activity and will have full authority as regards to its duties to ensure compliance with the provisions of the EU GDPR; Each local supervisory authority will still maintain in its own territory, and will monitor any local data processing that affects data subjects or that is carried out by an EU or non-EU controller or processor when their processing targets data subjects residing on its territory. Their tasks and powers includes conducting investigations and applying administrative measures and fines, promoting public awareness of the risks, rules, security, and rights in relation to the processing of personal data, as well as obtaining access to any premises of the controller and the processor, including any data processing equipment and means.

3. Basic Principles Regarding Personal Data Processing

3.1. Lawfulness, Fairness, and Transparency
Personal data must be processed lawfully, fairly, and in a transparent manner.

3.2. Purpose Limitation
Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.3. Data Minimization
Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. AJC must apply anonymization or pseudonymization to personal data if possible to reduce the risks to the data subjects.

3.4. Accuracy
Personal data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified in a timely manner.

3.5. Storage Period Limitation
Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed.

3.6. Integrity and Confidentiality
Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of personal data risks, AJC must use appropriate measures to process Personal Data in a manner that ensures appropriate security of personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

3.7. Accountability
Data controllers must be responsible for and be able to demonstrate compliance with the principles outlined above

4. Building Data Protection in Business

4.1. Notification to Data Subjects
When collecting or processing personal data, AJC will provide appropriate Privacy Notices to data subjects.

4.2. Data Subject's Choice and Consent
When collecting or processing personal data based on consent, AJC will act in accordance with the Fair Processing Guidelines contained in Section 6 below.

4.3. Collection
AJC must strive to collect the least amount of personal data possible. If personal data is collected from a third party, AJC must ensure that data is collected lawfully.

4.4. Use, Retention, and Disposal
The purposes, methods, storage limitation, and retention period of personal data must be consistent with the information contained in the Privacy Notice. AJC must maintain the accuracy, integrity, confidentiality, and relevance of personal data based on the processing purpose. Adequate security mechanisms designed to protect personal data must be used to prevent personal data from being stolen, misused, or abused, and prevent personal data breaches.

4.5. Disclosure to Third Parties
Whenever AJC uses a third-party supplier or business partner to process personal data on its behalf, AJC must ensure that this processor will provide security measures to safeguard personal data that are appropriate to the associated risks.

AJC must contractually require the supplier or business partner to provide the same level of data protection. The supplier or business partner must only process personal data to carry out its contractual obligations towards AJC or upon the instructions of AJC and not for any other purposes. When AJC processes personal data jointly with an independent third party, AJC must explicitly specify its respective responsibilities of and the third party in the relevant contract or any other legal binding document.

4.6. Cross-border Transfer of Personal Data
Before transferring personal data out of the European Economic Area (EEA), adequate safeguards must be used, including the signing of a Data Transfer Agreement as required by the European Union and, if required, authorization from the relevant Data Protection Authority must be obtained.

4.7. Rights of Access by Data Subjects
AJC is responsible to provide data subjects with a reasonable access mechanism to enable them to access their personal data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law.

4.8. Data Portability
Data Subjects have the right to receive, upon request, a copy of the data they provided to AJC in a structured format and to transmit those data to another controller, for free. AJC is responsible to ensure that such requests are processed within one month, are not excessive, and do not affect the rights of other individuals.

4.9. Right to be Forgotten
Upon request, Data Subjects have the right to obtain from AJC the erasure of its personal data, if appropriate or required by law. When AJC is acting as a Controller, AJC must take necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request.

5. Fair Processing Guidelines

Personal data must only be processed when explicitly authorised by the individuals within AJC responsive for data protection measures. AJC must decide whether to perform a Data Protection Impact Assessment for each processing activity.

5.1. Notices to Data Subjects
At the time of collection or before collecting personal data for any kind of processing activities, including but not limited to interviewing prospective candidates, managing employment, administering payroll and benefits, and contracting with applicable vendors, AJC is responsible to properly inform data subjects of the following: the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data (including their rights with respect to submitting complaints regarding the processing of their personal data), the retention period, potential international data transfers, if data will be shared with third parties, and the AJC's security measures to protect personal data. This information is provided through issuance of the appropriate Privacy Notice.

Where personal data is being shared with a third party, AJC must ensure that data subjects have been notified of this through issuance of the appropriate Privacy Notice for the type of data subject at issue. Where personal data is being transferred to a third country, the Privacy Notice should reflect this and clearly state to where, and to which entity personal data is being transferred.

Where sensitive personal data is being collected, AJC must make sure that the Privacy Notice explicitly states the purpose for which this sensitive personal data is being collected.

5.2. Obtaining Consents
Whenever personal data processing is based on the data subject's consent, or other lawful grounds, AJC is responsible for retaining a record of such consent. AJC is responsible for providing data subjects with options to provide the consent and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn at any time.

Where collection of personal data relates to a child under the age of 16, AJC must make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology, prior to the collection using the Parental Consent Form.

When a Data Subject requests to correct, amend, or destroy personal data records, AJC must ensure that these requests are handled within a reasonable time frame. AJC must also record the requests and keep a log of these.

Personal data must only be processed for the purpose for which they were originally collected. If AJC wants to process collected personal data for another purpose, AJC must seek the consent of its data subjects in clear and concise writing. Any such request should include the original purpose for which data was collected, and also the new, or additional, purpose(s).

The request must also include the reason for the change in purpose(s). Now and in the future, AJC must ensure that collection methods are compliant with relevant law, good practices, and industry standards.

6. Organization and Responsibilities

The responsibility for ensuring appropriate personal data processing lies with everyone who works for or with AJC and has access to personal data processed by AJC.

The managing director makes decisions about, and approves AJC's general strategies on personal data protection.

Several functions are responsible for managing the personal data protection program and are responsible for the development and promotion of end-to-end personal data protection policies.

These functions monitor and analyse personal data laws and changes to regulations, develop compliance requirements, and assist business departments in achieving their Personal data goals.

7. Guidelines for Establishing the Lead Supervisory Authority

Identifying a Lead Supervisory Authority is only relevant if AJC, which is not established in the UE, processes personal data in relation to the offering of goods or services to individuals in the EU, or monitors the behaviour of individuals within the EU.

8. Response to Personal Data Breach Incidents

When AJC learns of a suspected or actual personal data breach, AJC must perform an internal investigation and take appropriate remedial measures in a timely manner. Where there is any risk to the rights and freedoms of data subjects, AJC must notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.

9. Audit and Accountability

AJC is responsible for auditing how well its departments implement this Policy. Any employee who violates this Policy will be subject to disciplinary action in line with AJC policies, and may also be subject to sanctions or penalties under applicable law.

10. Conflicts of Law

This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which the AJC operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

11. Document Management

AJC must check and, if necessary, update this Policy at least once a year.