

Objective

The aim of this Privacy Policy ("Policy") is to provide adequate and consistent safeguards for the handling of candidate data by Island Joe Group (IJG).

The identifiable information about yourself that you provide to IJG as a job seeker for a position with IJG (the "Candidate Data" or "Data") will be used for recruitment purposes, and the Candidate Data will be protected in accordance with IJG's Policy outlined below and all applicable laws.

By submitting your Candidate Data, you confirm and agree that:

- you have reviewed IJG's Policy;
- IJG may process the Candidate Data according to the recruitment purposes set out in the Policy; and
- the Candidate Data may be transferred worldwide consistent with IJG's Policy

Your consent is required in order to complete the submittal process. If you do not agree, click on the "x" button in the upper right-hand corner and the submittal process will discontinue.

This Policy, unless noted otherwise, does not form part of any contract of employment, where applicable, offered to successful hires.

Scope

This Policy applies to all IJG that process Candidate Data.

Processing refers to any action that is performed on Candidate Data, whether in whole or in part by automated means, such as collecting, recording, organizing, storing, modifying, using, disclosing, or deleting such data.

Candidate Data are defined as any identifiable information about you that you or someone else provides (on your or IJG's behalf) in the context of applying for a position with IJG.

This Policy does not cover data rendered anonymous or where pseudonyms are used. Data are rendered anonymous if individual persons are no longer identifiable or are identifiable only with a disproportionately large expense in time, cost, or labor. The use of pseudonyms involves the replacement of names or other identifiers with substitutes, so that identification of individual persons is either impossible or at least rendered considerably more difficult. If Data rendered anonymous becomes no longer anonymous (i.e., individual persons are again identifiable), or if pseudonyms are used and the pseudonyms allow identification of individual persons, then This Policy will again apply.

Application of Local Laws

This Policy is designed to provide a uniform minimum compliant standard for every IJG entity with respect to its protection of Candidate Data worldwide. IJG recognizes that certain laws may require stricter policy than those described in This Policy. IJG will handle Candidate Data in accordance with local law applicable at the place where the Candidate Data are

processed. Where applicable local law provides a lower level of protection of Candidate Data than that established by This Policy, then the requirements of the Policy shall apply.

Principles for Processing Candidate Data

IJG respects the privacy rights and interests of each individual. IJG will observe the following principles when processing Candidate Data:

- Data will be processed fairly and lawfully
- Data will be collected for specified, legitimate purposes and not processed further in ways incompatible with those purposes
- Data will be relevant to and not excessive for the purposes for which they are collected and used. For example, Data may be rendered anonymous when feasible and appropriate, depending on the nature of the Data and the risks associated with the intended uses
- Data will be accurate and, where necessary, kept up-to-date. Reasonable steps will be taken to rectify or delete Candidate Data that is inaccurate or incomplete
- Data will be kept only as long as it is necessary for the purposes for which it was collected and processed
- Data will be processed in accordance with the individual's legal rights (as described in This Policy or as provided by law)
- Appropriate technical, physical, and organizational measures will be taken to prevent unauthorized access, unlawful processing, and unauthorized or accidental loss, destruction, or damage to Data

Data Collection

You may use various methods to submit your Candidate Data to IJG. These methods may include: (a) e-mail or paper submission to IJG personnel; (b) online submittal of Candidate Data processed by a third party service provider into an electronic database based in the U.S. accessible by IJG authorized personnel; or (c) via an IJG employment application.

IJG may periodically collect further information with your consent or in accordance with applicable laws. For example, IJG may collect your feedback and opinions (e.g., surveys) for business purposes, such as improving processes. You may respond to these surveys voluntarily or may elect not to respond and will not suffer reprisals for your decision. This Policy will be applicable to any further information collected including any responses to such surveys.

Purposes and Access for Candidate Data Processing

IJG processes Candidate Data for legitimate human resources purposes. Such processing will be conducted within such purpose limitations and in accordance with applicable law. These principal purposes include:

Human Resources Purposes Include: Identifying and/or evaluating candidates for IJG positions; making a decision about whether the individual should be hired; maintaining appropriate record-keeping related to hiring practices; analyzing the hiring process and outcomes; and conducting background investigations, where permitted by law (the "Purposes").

If IJG processes your Candidate Data for purposes that go beyond the Purposes described above, the IJG entity responsible for the new purpose will ensure that you are informed of the new purposes for which your Candidate Data are to be used, and the categories of recipients of your Candidate Data.

Your Data will be accessed and processed by individuals who are involved in the hiring process for IJG and who have a legitimate need to access and process your Data for the Purposes.

Types of Candidate Data

Candidate Data that is processed includes:

- Candidate status
- Work history/job data
- Education
- Compensation
- Employer feedback
- Online questionnaire results
- Candidate contact information
- Previous addresses or names of the Candidate
- Additional information provided by the Candidate (e.g., a cover letter)
- Driver's license number, as needed for certain positions
- References
- Criminal history, where permitted by law

Special Categories of Data

To the limited extent IJG needs to collect any Special Data (such as data containing personal information about racial or ethnic origin, political opinions, religious or political beliefs, trade-union membership, health or medical records, or criminal records), the IJG entity will ensure that the individual is informed of such collection and processing. Where required by law, the person's explicit consent to the processing and particularly to the transfer of such data to non-IJG will be obtained. Appropriate security and protection measures (e.g., physical security devices, encryption, and access restrictions) will be provided depending on the nature of these categories of data and the risks associated with the intended uses.

Security and Confidentiality

IJG are committed to taking appropriate technical, physical, and organizational measures to protect Candidate Data against unauthorized access, unlawful processing, accidental loss or damage, and unauthorized destruction.

Equipment and Information Security

To safeguard against unauthorized access to Candidate Data by third parties outside IJG, all electronic Candidate Data held by IJG are maintained on systems that are protected by secure network architectures that contain firewalls and intrusion detection devices. The servers holding Candidate Data are "backed up" (i.e., the data are recorded on separate media) on a

regular basis to avoid the consequences of any inadvertent erasure or destruction of data. The servers are stored in facilities with comprehensive security and fire detection and response systems.

Access Security

IJG limit access to internal systems that hold Candidate Data to a select group of authorized users who are given access to such systems through the use of a unique identifier and password. Access to Candidate Data is limited to and provided to individuals for the purpose of performing their job duties (e.g., a human resources manager may need access to a Candidate's contact information for the purposes of setting up an interview). Compliance with these provisions will be required of third-party administrators who may access certain Candidate Data, as described in the **Transferring Data** section.

Training

IJG will conduct training regarding the lawful and intended purposes of processing Candidate Data, the need to protect and keep information accurate and up-to-date, and the need to maintain the confidentiality of the Data to which employees have access. Authorized users will comply with This Policy, and IJG will take appropriate disciplinary actions, in accordance with applicable law, if Candidate Data are accessed, processed, or used in any way that is inconsistent with the requirements of This Policy.

Rights of Data Subjects

Any person may inquire as to the nature of the Candidate Data stored or processed about him or her by any IJG entity. You will be provided access to Candidate Data as is required by law in your home country, regardless of the location of the data processing and storage. IJG processing such data will cooperate in providing such access either directly or through another IJG entity. All such requests for access may be made by sending a request in writing to:

Human Resources Data Protection Administrator
19 N Court St, Ste 201
Frederick, MD 21701

Candidate Data will be available for access for a reasonable period of time, and IJG will allow you to view your Candidate Data upon reasonable notice and at reasonable times.

You may also contact the Human Resources Data Protection Administrator to ask questions regarding This Policy or your Candidate Data or withdraw your consent. Any letters sent to the Administrator for any other purpose other than the above will not be responded to and will be discarded.

If access or rectification is denied, the reason for the denial will be communicated and a written record will be made of the request and reason for denial.

If you demonstrate that the purpose for which the data is being processed is no longer legal or appropriate, the data will be deleted, unless the law requires otherwise.

If any Candidate Data is inaccurate or incomplete, you may request that the data be amended by submitting a new resume/CV with the updated information (e.g., new home address or change of name).

Transferring Data

Transfers to other IJG

IJG strives to ensure a consistent and adequate level of protection for Candidate Data that are processed and/or transferred between IJG. A transfer of Candidate Data to another IJG entity is considered a transfer between two different entities, which means that even in such “intra-group” cases, a data transfer shall be carried out only if applicable legal requirements are met and if:

- The transfer is based on a clear business need;
- The receiving entity provides appropriate security for the data; and
- The receiving entity ensures compliance with This Policy for the transfer and any subsequent processing

Transfers to non-IJG

- **Selected Third Parties:** At times, IJG may be required to transfer Candidate Data to selected external third parties that they have hired to perform certain employment-related services on their behalf. These third parties may process the data in accordance with the IJG entity’s instructions or make decisions regarding the data as part of the delivery of their services. In either instance, IJG will select reliable suppliers who undertake, by contract or other legally binding and permissible means, to put in place appropriate security measures to ensure an adequate level of protection. IJG will require external third-party suppliers to comply with This Policy or to guarantee the same levels of protection as IJG when handling Candidate Data. Such selected third parties will have access to Candidate Data solely for the purposes of performing the services specified in the applicable service contract. If IJG concludes that a supplier is not complying with these obligations, it will promptly take appropriate actions
- **Other Third Parties:** IJG may be required to disclose certain Candidate Data to other third parties (1) as a matter of law (e.g., to tax and social security authorities); (2) to protect IJG’s legal rights (e.g., to defend a litigation suit); or (3) in an emergency where the health or security of a Candidate is endangered (e.g., a fire)

Direct Marketing

IJG will not disclose Candidate Data outside IJG to offer any products or services to a Candidate for personal or familial consumption (“direct marketing”) without his or her prior consent.

The restrictions in this section apply only to contact data obtained in the context of applying for a position with IJG. They do not apply to contact data obtained in the context of a consumer or customer relationship.

Automated Decisions

Some countries regulate the making of Automated Decisions, which are decisions about individuals that are based solely on the automated processing of data and that produce legal effects that significantly affect the individuals involved.

In some circumstances, job seekers will be asked to complete a questionnaire where automated decisions will be made based on the Candidate's responses.

Except in limited circumstances (e.g., the screening via computer or telephone for some open positions in IJG), IJG do not make Automated Decisions to evaluate individuals or for other purposes. If Automated Decisions are made, affected persons will be given an opportunity to express their views on the Automated Decision in question by contacting the Human Resources Data Protection Administrator.

Enforcement Rights and Mechanisms

All IJG will ensure that This Policy is observed. All persons who have access to Candidate Data must comply with This Policy. In some countries, violations of data protection regulations may lead to penalties and/or claims for damages.

If at any time, a person believes that Candidate Data relating to him or her has been processed in violation of This Policy, he or she may report the concern to the Human Resources Data Protection Administrator.

If the concern relates to an alleged violation of This Policy by IJG located in a country other than that of the person or the exporting IJG entity, he or she may request the assistance of the exporting entity. That IJG entity will assist him or her in investigating the circumstances of the alleged violation. If the violation is confirmed, the exporting and importing entities will work together with any other relevant parties to resolve the matter in a satisfactory manner, consistent with the provisions of This Policy.

If the Human Resources Data Protection Administrator or the local IJG entity does not resolve the concern, it may be escalated to IJG's CEO. The Employment Data Privacy Committee will communicate its decision and any associated remedy to the relevant persons.

The processes described in This Policy supplement any other remedies and dispute resolution processes provided by IJG and/or available under applicable law.

Audit Procedures

To further ensure enforcement of This Policy, IJG's CEO will identify Candidate and employment Data procedures that should be audited. For this purpose, IJG will engage its Corporate Audit Committee, composed of IJG's outside legal counsel, outside HR consulting firm, and outside Accounting firm, who are independent of IJG's management. Members of the Audit Committee report to IJG's CEO. Reports of the Audit Staff's findings will be submitted to IJG's CEO. The CEO will require an action plan to ensure compliance with This Policy. To the extent such matters cannot be adequately handled with IJG's own resources, IJG agrees to appoint an independent third party to conduct an investigation/audit of any procedures or issues involving Candidate or employment Data under the Policy.

Communication About the Policy

In addition to the training on This Policy, IJG will communicate This Policy to current and new employees by posting them on selected internal IJG web sites and by providing a link to the Policy on information technology applications where Candidate Data are collected or processed.

Modifications to the Policy

IJG reserves the right to modify This Policy as needed, for example, to comply with changes in laws, regulations, IJG practices and procedures, or requirements imposed by data protection authorities. IJG's Chief Privacy Leader, or his/her designee, must approve all changes to the Policy for them to become effective. If IJG makes changes to the Policy, IJG will submit the Policy for renewed approval where required by law. IJG will inform IJG employees and other persons (e.g., persons accessing IJG web sites to enter Candidate Data such as job application information) of any material changes in the Policy. IJG will post all changes to the Policy on relevant internal and external web sites.

Effective with the implementation of This Policy, all existing intra-group agreements and applicable company privacy guidelines relating to the processing of Candidate Data will be superseded by the terms of This Policy. All parties to any such agreements will be notified of the effective date of implementation of the Policy.

Obligations Toward Data Protection Authorities

IJG will respond diligently and appropriately to requests from data protection authorities about This Policy or compliance with applicable data protection and privacy laws and regulations. IJG employees who receive such requests should contact their local Human Resources manager or business legal counsel. IJG will, upon request, provide data protection authorities with names and contact details of relevant contact persons. With regard to transfers of Candidate Data between IJG, the importing and exporting IJG will (i) co-operate with inquiries from the data protection authority responsible for the entity exporting the data, and (ii) respect its decisions, consistent with applicable law and due process rights.

Addendum

Rights and Obligations with Respect to Candidate Data Collected Within the EU/EEA and Processed Elsewhere

In addition to any rights and obligations that are set forth in IJG's Candidate Data Protection Policy ("Policy") or that otherwise exist, the following principles established in light of Directive 95/46/EC ("European Data Protection Directive") will apply to Candidate Data collected by IJG in the European Union/European Economic Area and processed elsewhere. In jurisdictions where this Addendum applies, the enforcement rights and mechanisms mentioned in the Policy also apply to the provisions of this Addendum. The following are not intended to grant employees further rights or establish further obligations beyond those already provided under the European Data Protection Directive:

1. Job seekers may object to the processing of Candidate Data about them on compelling legitimate grounds relating to their particular situation. This might occur, for instance, if the job seeker's life or health is at risk due to the processing of the data. This provision shall not apply if the processing is (i) required by law, (ii) based on the job seeker's individual consent, or (iii) necessary to fulfill a contractual obligation between the job seeker and IJG
2. After exhausting appropriate internal dispute resolution processes, job seekers may seek compensatory damages from IJG for loss or damage to them caused by a violation of the Policy (including the provisions of this Addendum)

by the IJG entity. The IJG entity shall not be liable for damages if it has observed the standard of care appropriate in the circumstances

3. If any of the terms or definitions used in the Policy are ambiguous, the definitions established under applicable local law within the relevant EU/EEA member state shall apply or where there are no such definitions under applicable local law, the definitions of the European Data Protection Directive shall apply.