Text Recruit – Legal

PRIVACY POLICY

Policy Document

DOCUMENT INFORMATION AND APPROVALS

VERSION HISTORY			
Version #	**Date**	**Revised By**	**Reason for change**
0.0	03/30/2018	Shivani Malik	Initial Privacy Policy
1.0	05/02/2018	Shivan Malik	Final Draft

DOCUMENT APPROVALS AND STAKEHOLDERS					
Name	**Title**	**Department**	**Role**	**Signature**	**Date**
Courtney Dutter	**Assistant General Counsel**	**Legal**	**Approver**		

1. Document Purpose

This Privacy Policy (the "Policy") delineates Text Recruit's (the "Company") commitment to the principles of data protection and the need to balance the rights of individuals with the functions and operational requirements of the Company. This Policy applies to all Sensitive and/or Confidential Information managed by the Company regardless of the media on which the data is stored. The Company manages the Sensitive and/or Confidential Information of our customers, vendors, employees, and other applicable third parties in accordance with U.S. laws requiring the protection of data, including the United States Privacy Act, as well as international regulations like the EU's General Data Protection Regulation, and privacy best practices.

This Policy and related policies and procedures are internal documents and should not be shared or distributed to third parties, customers or regulators without the prior authorization of the Office of the Data Protection Steward ("ODPS").

Printed documents are uncontrolled. Refer to 'Watercooler – Employee Resources – Process Documents' for controlled versions.

2. Glossary of Terms

Term/Acronym	Definition
Automated Decision-Making (ADM)	means when a decision is made solely on the basis of Automated Processing.
Automated Processing	means any computerized processing of Personal Data to evaluate certain aspects relating to an individual, including analysis or predictions concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Profiling is an example of Automated Processing.
Confidential Information	means non-public information that derives independent value from not being generally known to the public, but does not include any information that (i) was or subsequently becomes publicly available without breach of any confidentiality obligations, (ii) was known prior to the disclosure of such information, (iii) was or is subsequently obtained from another source without breach of any confidentiality obligation, or (iv) is independently developed without reference to any Sensitive and/or Confidential Information.
Confidentiality Obligations	means confidentiality agreements, or terms within employment, consulting, subscription, software, services, distributor, and other agreements that Text Recruit executes with Personnel or NKPs that define the nature of Sensitive and/or Confidential Information, the rights and obligations with respect to such Sensitive and/or Confidential Information, and proper handling procedures associated with such Sensitive and/or Confidential Information.
Consent	means a statement or a clear positive action, performed by the Data Subject, that signifies their agreement to the Processing of their Personal Data. This consent should be freely given, specific, informed, and be an unambiguous indication of the Data Subject's wishes.
Data Breach	*Please refer to the Text Recruit's Incident Response Policy.*
Data Controller	means the person or organization that determines the purpose and means of the Processing of Personal Data.
Data Processor	means the person or organization that Processes Personal Data.
Data Subject	means a living, identified or identifiable individual for whom the Company holds Sensitive and/or Confidential Information. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.
Dispose	and its cognates mean the discarding or abandonment of Sensitive and/or Confidential Information; or the sale, donation, or transfer of any medium, including computer equipment, upon which this Sensitive and/or Confidential Information is stored.

Term/Acronym	Definition
Explicit Consent	means Consent which requires a very clear and specific statement not just an action.
GDPR	means the Regulation (EU) 2016/679 on the protection of natural persons with regard to Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Need to Know Parties (NKP)	*Please refer to the Text Recruit's PIM Policy.*
Office of the Data Protection Steward (ODPS)	means the team established within Text Recruit to manage, inform, monitor, advise, and/or analyze the privacy implications and ensure compliance with applicable national and international regulations on privacy and security and establish a Personal Data management system to assist the Company in implementing protections to provide outstanding customer service for its clients.
Personal Data	*Please refer to the Text Recruit's PIM Policy.*
Personal Identifiable Information (PII)	*Please refer to the Text Recruit's PIM Policy.*
Personnel	means Text Recruit employees (part-time and full-time), interns, directors, and members.
Privacy Impact Assessment (PIA)	*Please refer to the Text Recruit's PIM Policy.*
Privacy Shield Framework	means the framework administered by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Economic Area to the United States.
Privacy Shield Principles	means the seven core principles of data protection that companies must implement in order to certify for the Privacy Shield Framework, and the sixteen supplemental principles.
Process	and its cognates mean any operation or set of operations which is performed on Personal Data, whether or not by automatic means, such as collection, recording organization, structuring, storage, adaption or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	means a specific NKP that Processes Personnel data with respect to Text Recruit's corporate operations.
Security Incident	*Please refer to the Text Recruit's Incident Response Policy.*
Sensitive Company Information (SCI)	*Please refer to the Text Recruit's PIM Policy.*
Sensitive Information	*Please refer to the Text Recruit's PIM Policy.*
Sensitive Personal Data (SPD)	*Please refer to the Text Recruit's PIM Policy.*
Sensitive Personal Information (SPI)	*Please refer to the Text Recruit's PIM Policy.*
Subject Access Request (SAR)	means a request by a Data Subject, under GDPR, to be informed by the Data Controller of the following: (i) what Personal Data is being processed; (ii) the purpose for which the Personal Data is being processed; (iii) who, if anyone, the Personal Data is disclosed to; and (iv) the extent to which it is using Personal Data for the purpose of making automated decisions relating to the data subject, and if so, what logic is being used for that purpose.
Sub-Processor	means a specific NKP that processes customer Personal Data in connection with any product or service delivered by Text Recruit, including the Text Recruit Talent Platform.
Tracking Data	*Please refer to the Text Recruit's PIM Policy.*

3. Overview and Background

The Company recognizes the importance of data privacy and adopts this formal Policy to ensure that Sensitive and Confidential Information, including Personal Data as defined by the European Union's (EU) General Data Protection Regulation (GDPR), is gathered, used, stored, shared, protected, retained, and disposed of in accordance with applicable data protection regulations, privacy best practices, and the Company's policies and procedures. To this end, Text Recruit has adopted this Policy and the corresponding PIM Policy designed to address how Sensitive and Confidential Information, including Personal Data, are protected under applicable national or international regulations and best practices:

4. Ownership & Administration

5.1. This Policy is owned by the iCIMS General Counsel's Office ("GCO").

5.2. This Policy is administered by Text Recruit.

5.3. The ODPS may be contacted by emailing privacy@icims.com.

6. Applicability

6.1. This Policy applies to Personnel, NKPs, Processors, and Sub-processors.

6.2. This Policy applies to the lawful processing of all customer data.

6.3. This Policy supersedes all other policies, procedures, practices, and guidelines relating to the matters set forth herein.

6.4. All employees, users, agents, and assigns of Personnel, NKPs, Processors, and Sub-processors shall abide by this Policy.

7. Scope

The Company recognizes that protecting the confidentiality and integrity of information is a critical responsibility. The Company takes this responsibility seriously and expects that Personnel and NKPs adhere to this Policy when handling Sensitive and Confidential Information in order to provide successful business operations and maintain confidence in Text Recruit' technology and services.

7.1. **In Scope**

- This Policy applies to all Sensitive and Confidential Information obtained by the Company through its platform on behalf of its subscribers for Processing.
- This Policy applies to all Sensitive and Confidential Information obtained by the Company through its platform on behalf of its Personnel as a Data Controller.
- This Policy applies to all Sensitive and Confidential Information as obtained by the Company in the course of business and the employment of Personnel.
- This Policy applies to all Sensitive and Confidential Information Processed on behalf of the Company through Personnel and/or NKPs.
- This Policy applies to the Processing of Personal Data in accordance with the Processing of EU residents' information under GDPR.
- This Policy applies to the Processing of all Personal Data in accordance with the Processing of U.K. residents' information under GDPR and as aligned with the U.K. Data Protection Bill.

7.2. **Out of Scope**

- This Policy does not apply to Sensitive and/or Confidential Information Processed by customers as a Data Controller outside of the Company's platform.

8. Roles and Responsibilities

Text Recruit takes a top down approach to the privacy of information to ensure that data protection regulations and principles emanate throughout the Company. Text Recruit Executive Officers, are responsible for compliance with this Policy and implementation of appropriate practices, processes, controls, and training to ensure compliance within each department.

8.1. **Office of the Data Protection Steward (ODPS)**

8.1.1. Office of the Data Protection Steward (ODPS) – The ODPS is comprised of iCIM's legal, compliance, privacy, and security roles working in conjunction with the Text Recruit Executive Officer to oversee this Policy and developing related privacy and security policies, standards, procedures, and/or guidelines to maintain the privacy program throughout the Company.

8.1.2. Text Recruit Executive Officers

8.1.3.

The ODPS is the central point of contact for all questions and concerns about the operation of this Policy, GDPR, and all other applicable laws, rules, regulations, and best practices as they relate to the Company's privacy program. Additionally, the ODPS works as a team and Text Recruit Executive Officers to ensure that the Company's privacy principles are being implemented accordingly.

Name: ODPS
Email Address: privacy@icims.com

If direction has not already been provided by the ODPS in the form of a policy, process, standard or guideline the ODPS ***must*** be contacted in the following circumstances when dealing with Personal Data under the GDPR:

(a) If there has been a Data Breach, as further provided in Section 9.1.7 below.
(b) Directions from a Data Controller are in direct contradiction to GDPR and/or other privacy laws or regulations.
(c) There is a question or concern as to the lawful basis which you are relying on to Process Personal Data, including the legitimate interests of the Company.
(d) Consent is needed and/or Explicit Consent must be captured and is currently not being obtained or captured during the process.
(e) Privacy notices and/or Processing notices need to be drafted.
(f) There is a question or concern regarding the retention period for the Personal Data processed.
(g) There is a question or concern about what security measure or other protection measure needs to be implemented to protect Personal Data.
(h) There is a question or concern regarding the transfer or sub-processing of Personal Data outside of the European Economic Area (EEA)
(i) There is a question or concern regarding providing assistance to a Data Subject that has invoked his/her rights under GDPR.

(j) A new Personal Data Processing activity is being developed or a significant Personal Data Processing activity change is being implemented.
(k) A change in the use of Personal Data for purposes other than what it was collected for.
(l) An activity that involves Automated Processing, including profiling or Automated Decision Making, of Personal Data.
(m) To ensure compliance with national and international data privacy law if direct marketing activities are being carried out.
(n) Sharing Personal Data with Personnel, NKPs, Processors, or Sub-Processors.

9. GDPR Privacy Principles

In the normal course of business, the Company and its Personnel may create, receive, store, maintain, process, or otherwise access information.

The Company adheres to the data privacy regulations issued by the EU under GDPR for all Personal Data, including SPD and Tracking Data. To this end, the Company recognizes Personal Data is the property of the Data Subject and regards the lawful, correct, and secured treatment of Personal Data as extremely important. The Company implements the following principles of data protection for all Personal Data processed by the Company under GDPR for EU residents:

1. Personal Data is obtained and Processed fairly and lawfully and shall not be Processed unless the Processing is necessary for the purposes defined under applicable regulation
2. Personal Data is obtained for one or more lawful purposes and not Processed in a manner incompatible with that purpose.
3. Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal Data is accurate and kept up to date
5. Personal Data should not be kept for longer than is necessary for that purpose.
6. Personal Data shall be Processed in accordance with the rights of the Data Subject.
7. Personal Data shall be treated as Sensitive Information and appropriate technical and organizational safeguards shall be implemented to prevent unauthorized or unlawful Processing and access of Personal Data as well as accidental loss or destruction or damage to Personal Data.

9.1. GDPR Personal Data Protection Guidelines

9.1.1. Lawful, Fair, and Transparent Processing

- Processing information is provided at the time Personal Data is collected from the Data Subject.
- When collecting Personal Data, the Company informs Data Subjects about why their Personal Data is required and how it will be used and retained. It also explains whether the Personal Data is shared.
- The Company does not Process Personal Data using ADM.

- Upon request from the Data Subject, by and through the Data Controller, the Company, will provide details surrounding the Processing of Personal Data. This is known as a Subject Access Request (SAR).
- Processing Personal Data must be approved by the ODPS and documented within the relevant PIA.

9.1.2. Purpose Limitation

- The Company will only Process Personal Data that it actually needs to fulfill its business and operational requirements.
- The Company recognizes that Personal Data collected may be used in different ways, if it is deemed appropriate and fair. In such cases, the Data Subject will be advised if their Personal Data is to be used in a new way.

9.1.3. Disclosing Personal Data

- The Company works with other organizations to provide services. The sharing of Personal Data between the Company and third parties is subject to formal information sharing protocols. These protocols are common rules adopted by the Company and its third-parties with whom it wishes to share data.
- The details of each data sharing process are documented in official agreements.
- All new data sharing protocols and agreements should be approved by the GCO.
- Personal Data will only be transferred to Processors and Sub-processors under circumstances where the Personal Data can be adequately protected.
- There are numerous instances where it will be fair and reasonable to disclose Personal Data with and without the consent of the Data Subject. All requests for Personal Data and disclosures must be documented.
- Information may be shared through partnership arrangements where there is a data sharing agreement in place or where the Data Subject has authorized disclosure through a mandate.
- If the Company discloses Personal Data, it will only disclose necessary Personal Data for the stated purpose.
- Unauthorized disclosure of Personal Data is strictly prohibited. Personnel and NKPs, Processors, and Sub-processors should not disclose Personal Data obtained in the course of their work with the Company, or access Personal Data without appropriate permissions. Before obtaining or disclosing Personal Data the consent of the Data Controller should be obtained as severe legal penalties may result without such consent.

9.1.4. Accurate Processing

- The Company has compiled and implemented policies and processes to address how it maintains the Personal Data it Processes.
- The Company distributes data protection obligations to its customers to inform them how it maintains the Personal Data it Processes on their behalf.

9.1.5. Privacy by Design

- The Company embeds privacy considerations into business processes and systems through appropriate physical, technological, and procedural controls reasonably designed to ensure Personal Data is secured in accordance with the GDPR.
- Upon the implementation of a new system or a significant update to an existing system that uses Personal Data, the ODPS will implement the Privacy Impact Assessment (PIA) process revealing whether there are high risk Processing activities that require consultation with the Supervisory Authority.

9.1.6. Limitation of Storage

- All Personal Data must be disposed of in accordance with the IT Security Policy and Data Security & Privacy Statement.
- The Company's information security policies and procedures must be followed at all times with, particular focus on the storage and transportation of Personal Data, to ensure that unauthorized access or disclosure does not happen by accident or design.

9.1.7. Accountability and Liability

- A Data Breach can occur through malicious acts or accidently.
- In accordance with the Incident Response Procedures, the SIRT will determine if a Security Incident involving a Data Breach has occurred and will notify the ODPS.
- Upon notification the ODPS will notify the proper authorities and parties in accordance with applicable regulation.

10. **Sensitive and/or Confidential Information Privacy Standards**

The Company adheres to the following data privacy principles for all Sensitive and/or Confidential Information, including Personal Data.

- Physical and Procedural Safeguards –
  - Text Recruit implements physical measures to prevent unauthorized entry to our premises and secured areas, as well as unauthorized access to our Sensitive and/or Confidential Information. Please refer to the Company's IT Security Policy and Data Retention Schedule for further explanation.
  - Text Recruit implements privacy and security processes that are aligned with this Policy to protect Sensitive and/or Confidential Information.
    - The Business Continuity Plan
    - The Incident Response Policy
    - The Data Security and Privacy Policy
    - The Employee Handbook
    - If Personnel encounter information, documents or other materials, whether disclosed in writing or orally, for which there is some doubt as to whether it should be treated as Sensitive and/or Confidential Information, or how it can be disclosed or used he or she shall:

    - Treat such information, documents or materials as Sensitive and/or Confidential Information governed by this Policy; and/or
    - Contact the GCO who shall make a joint determination on how best to proceed.
- Computer and Network Safeguards – Text Recruit adopts the IT Security Policy and other security policies and standards, to protect the integrity of our computer systems and protect Sensitive and/or Confidential Information from interference, unauthorized access, modification, and disclosure.