Text Recruit – Legal

DATA SECURITY & PRIVACY STATEMENT[1]

Statement Document

DOCUMENT INFORMATION AND APPROVALS

Version 1.0, 5/10/2018

[1] This Statement supersedes and replaces the privacy statement previously referred to as the Data Security & Privacy Policy.

1. GLOSSARY OF TERMS

Term/Acronym	Definition
Automated Decision-Making (ADM)	means when a decision is made solely on the basis 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.
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' 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.
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)	means Text Recruit consultants, vendors, partners, or other third parties that are provided Information by Text Recruit on a need-to-know basis subject to confidentiality obligations.
Personal Data	means any information relating to an identified or identifiable Data Subject, where such information is protected under applicable law. For clarity, Personal Data includes any SPD, SPI, and/or Tracking Data that directly or indirectly identifies a Data Subject.
Personal Identifiable Information (PII)	means any information about a Data Subject, whether in paper, electronic, or other form, which can be used to distinguish or trace an individual's identity, such as name, email address, or telephone number
Personnel	means Text Recruit employees (part-time and full-time), interns, directors, and members.
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' corporate operations.
Security Incident	*Please refer to the Text Recruit' Incident Response Policy.*
Sensitive Personal Information (SPI)	means specific standalone PII or a combination of information that could identify, trace, or locate a Data subject, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.
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.

2. TEXT RECRUIT'S COMMITMENT TO PRIVACY

Text Recruit recognizes the importance of protecting and ensuring the integrity of Sensitive and Confidential Information, including Personal Data as defined by the European Union's (EU)

General Data Protection Regulation (GDPR). Sensitive and Confidential Information is gathered, used, stored, shared, secured, retained, and disposed of in accordance with applicable data protection regulations, privacy best practices, and the terms of the agreement between Text Recruit and the subscriber.

This Statement explains how we process, gather, use, store, share, secure, retain, and dispose of Sensitive and Confidential information, including Personal Data on behalf of our subscribers' and their users.

Any questions regarding this Policy and our privacy practices should be sent by email to privacy@icims.com or by writing to the attention of Privacy Officer, iCIMS, Inc., 101 Crawfords Corner Rd. Suite 3-100, Holmdel, NJ 07733.

3. WHO ARE WE?

Text Recruit delivers a tool that allows subscribers to send text messages as part of the talent acquisition lifecycle or for other employment purposes as determined by the subscriber. Text Recruit is dedicated to meeting the privacy and data protection needs of its subscribers, in order to protect Sensitive and Confidential Information for our subscribers' users

4. TYPES OF SENSITIVE INFORMATION PROCESSED

Text Recruit processes information on behalf of its subscribers. The type of information generally processed by Text Recruit includes the following categories of data.

- First Name
- Last Name
- Telephone number
- Content of text message sent by the subscriber to the subscribers' users.[2]

To this end, Text Recruit recognizes that processing Sensitive Information varies by country and implements the following principles of data protection based upon the agreement between the subscriber and Text Recruit, and the subscriber's requirements.

4.1. PERSONAL DATA

Text Recruit processes Personal Data as defined by the EU GDPR on behalf of its subscribers. Personal Data includes the following data types: Internal Data; External Data; Financial Data; Social Data; Historical Data; and Tracking Data.

Examples of Types of Personal Data

Internal Data	External Data	Financial Data	Social Data	Historical Data	Tracking Data
○ Religious or Philosophical Beliefs ○ Passwords ○ PINs ○ Mother's Maiden Name ○ Opinions ○ Intentions ○ Interests ○ Likes/Dislikes	○ Name ○ Username ○ Unique Identifier ○ Gov't Issued Identification ○ Picture ○ Biometric Data ○ Ethnicity/Race ○ Spoken Language	○ Credit Card Number ○ Bank Account Number ○ Automobile Ownership ○ Home Ownership ○ Apartment Rentals	○ Job Titles ○ Work History ○ School Attended ○ Employee Records ○ Employment History ○ Evaluations ○ References ○ Interviews	○ Information about an individual's personal history (e.g., whether they were part of 9/11, WWI, WWII)	○ IP Address ○ MAC Address ○ Browser Fingerprint ○ Email Address ○ Physical Address ○ Telephone Number ○ Country

[2] Text Recruit does not govern the content of text messages. The content of text messages is controlled by the privacy practices of the subscriber.

	○ Sex Life or Orientation ○ Browsing Behavior ○ Call Logs ○ Links Clicked ○ Demeanor/ Attitude ○ Demographic Information ○ Medical or Health Information ○ Physical Characteristics	○ Personal Possessions ○ Credit Report ○ Sales and Purchases ○ Loan Records ○ Spending Habits ○ Taxes ○ Credit Worthiness ○ Credit Score ○ Credit Capacity	○ Certifications ○ Disciplinary Actions		○ GPS coordinates ○ Electronic Room Number

4.2. SENSITIVE PERSONAL INFORMATION (SPI)

Text Recruit may process SPI on behalf of its subscribers through the content of a text message, however, the content of text messages is controlled by the privacy practices of the subscriber so please refer to the applicable subscriber's privacy practices.

SPI is a narrow form of Personal Identifiable Information (PII), which is a U.S. privacy term used to describe sensitive or non-sensitive information that can identify an individual. SPI includes information that when disclosed could result in harm, embarrassment, inconvenience, or unfairness to the individual. SPI can originate from financial information, health information, or electronic communication, such as a bank account number or fingerprint. Additionally, SPI can be derived by a combination of information such as the last four digits of a social security number coupled with a date of birth. For clarity, SPI does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records, lawfully made available to the general public.

Examples of Types of SPI

Stand Alone PII	Combination Types if Paired with Another Type of PII
○ Non-truncated Social Security ○ Driver's license or state ID number ○ Passport number ○ Alien Registration Number ○ Financial account number ○ Biometric identifiers	○ Citizenship or immigration ○ Medical Information ○ Ethnic or religious affiliation ○ Sexual orientation ○ Account passwords ○ Last 4 digits of SSN ○ Date of birth ○ Criminal history ○ Mother's maiden name

5. How We Process Confidential and Sensitive Information

Personnel and NKPs shall only use Confidential and Sensitive Information for a legitimate business purpose in the performance of their duties, including (without limitation):

- To provide the Subscription to subscribers and their users or as otherwise permitted by a subscriber in its agreement with Text Recruit;
- To support Text Recruit's quality, security, and "customer experience" improvement initiatives.

5.1. Processing of Personal Data

Text Recruit recognizes that Personal Data is the property of the Data Subject and regards the lawful, correct, and secured treatment of Personal Data as extremely important. Text Recruit implements the following principles of data protection for all Personal Data processed by Text Recruit under GDPR for EU or U.K. 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 GDPR.
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.

These principles must be followed at all times when Processing or using Personal Data. Through appropriate management and strict application of criteria and controls Text Recruit:

1. Observes the fair collection and use of Personal Data by giving consent or having legitimate grounds for Processing the information.
2. Delivers notification of how your information is Processed at the time Personal Data is collected from the Data Subject.
3. Provides notification to the Data Subject explaining why their Personal Data is required and how it will be used and retained. It also explains whether the Personal Data is shared.

4. Does not Process Personal Data using ADM.
5. Ensures that the rights of people about whom information is held can be fully exercised under the GDPR.
6. Processes Personal Data to fulfill its business and operational requirements.
7. Advises the Data Subject if their Personal Data is to be used in a new way.
8. Ensures that sharing of Personal Data with third parties is subject to formal information sharing protocols and the details of each data sharing process are documented in official agreements.
9. Transfers information to Processors and Sub-processors under circumstances where the Personal Data can be adequately protected.
10. Documents all requests and disclosures of Personal Data.
11. Information shared through partnership arrangements will be governed by a data sharing agreement or where the Data Subject has authorized disclosure through a mandate.
12. Disclosure of Personal Data is for the stated purpose.

5.1.1. Subject Access Rights

Under the GDPR a Data Subject may request details about his/her Personal Data which Text Recruit processes on behalf of a subscriber and their users. These rights include: the right to be informed that processing is being undertaken, to access one's personal information, to prevent processing in certain circumstances, and to correct, rectify, block, or erase information that is regarded as incorrect.

Text Recruit assists its subscribers in fulfilling Subject Access Requests in accordance with the terms of the agreement between Text Recruit and the subscriber.

5.2. Privacy By Design

Text Recruit 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.

Text Recruit implements various security measures through its information security policies and procedures that ensures that unauthorized access or disclosure of Sensitive and/or Confidential Information does not happen by accident or design.

6. Safeguarding of Confidential and Sensitive Information

In addition to processing Personal Data in accordance with the principles of the GDPR, Text Recruit adheres to the following data privacy principles for all Sensitive and/or Confidential Information, including PII and SPI. To this end Text Recruit, implements physical, procedural, and information technology safeguards as follows:

1. Text Recruit configures its outgoing email transmissions to include the General Counsel's Office approved unintended recipient confidentiality language.
2. 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.
3. Text Recruit uses an access control system to restrict and monitor the Text Recruit's' premise and secured areas.

4. Text Recruit shall use reasonable efforts to ensure all visitors are authorized before entering the iCIMS premises and areas where Sensitive and/or Confidential Information is processed or maintained, including, but not limited to, taking the following actions as appropriate:
    a. Providing visitors a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-Personnel;
    b. Asking visitors to surrender the physical token before leaving the facility or at the date of expiration;
    c. Documenting procedures to help all Personnel easily distinguish between Personnel and visitors, especially in areas where Sensitive Information is accessible.
5. Text Recruit shall use reasonable efforts to maintain a physical audit trail of visitor activity, including, but not limited to, documenting the visitor's name, the firm represented, and Personnel authorizing physical access on the log. Logs should be kept for a minimum of three months unless otherwise restricted by law.
6. Access to areas containing sensitive material and stored items, including personal records, financial records, office supplies, and computer equipment are restricted and monitored.
7. Text Recruit implements and maintains security practices on its IT systems, including network, equipment, and communication systems supporting Text Recruit's internal and remote operations and Text Recruit-hosted products and services, including, but not limited to, encryption, virus protection, access controls, firewall egress and ingress, and LAN/WAN security. *See* IT Security Policy for further details.

7. RESPONSIBILITIES OF PERSONNEL

Unauthorized disclosure of Sensitive and Confidential Information is strictly prohibited. Personnel, Processors, and Sub-processors should not disclose Sensitive and Confidential Information obtained in the course of their work with Text Recruit, or access Sensitive and Confidential Information without appropriate permissions. The terms of the agreement between Text Recruit and the subscriber dictates how Sensitive and Confidential Information is obtained and/or disclosed.

Personnel shall use reasonable efforts to safeguard Sensitive and Confidential Information and keep it private and confidential, including, but not limited to, taking the following actions as appropriate:

1. Only sharing Information with authorized Personnel and NKP who "need to know" such Information for a legitimate business purpose in the performance of their authorized duties;
2. Only storing all electronic Sensitive and Confidential Information in secured equipment or devices (e.g., using a unique password or biometric security measure for Windows login, Outlook login, and/or directory or file access);
3. Only storing paper Sensitive and Confidential Information in a locked drawer or office (i.e., not leaving documents lying openly on desks);
4. Not sharing unique passwords and updating existing passwords on a periodic basis;
5. Properly labeling and/or segregating Sensitive and Confidential Information belonging to one party from information belonging to another party;
6. Not storing any Sensitive Information on any laptop or portable device unless it has been confirmed that such Sensitive Information is encrypted on such equipment or device;

7. Not transmitting any Personal Data and/or Sensitive Personal Information from a non-iCIMS mail server (e.g., personal Gmail, Yahoo!, or Hotmail account).
8. Not leaving any unsecured Sensitive and/or Confidential Information, or unsecured equipment or devices containing Sensitive and/or Confidential Information unattended or in an unsecured area.
9. Using reasonable efforts to Dispose of Sensitive and/or Confidential Information when such Information is no longer needed, and shall obtain the return of Sensitive and/or or Information from an NKP when it no longer needs such Information or it is no longer an authorized NKP.
10. 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 Confidential or Sensitive Information, or how it can be disclosed or used he or she shall:
    a. Treat such information, documents, or materials as Confidential and/or Sensitive Information as provided herein; and/or
    b. Contact the Office of the Data Protection Steward, who shall make a joint determination on how best to proceed.

8. Disposal of Information

1. All Sensitive and/or Confidential Information, including Personal Data, PII, and SPI, must be Disposed of in accordance with applicable regulations and iCIMS' policies and procedures that control the Disposal of Sensitive and/or Confidential Information.
2. When Disposing of Information, Personnel and NKPs shall take reasonable measures to protect against unauthorized access to or use of the Information in connection with its Disposal. Examples of such reasonable measures include, but are not limited to, any of the following:
    a. Burning, pulverizing, or shredding of papers or records containing Information so that the Information cannot be practicably read or reconstructed;
    b. Destroying or erasing electronic media containing Information so that the Information cannot practicably be read or reconstructed, consistent with reasonable standards.

9. Accountability and Liability

1. The GCO shall monitor compliance with this Policy through periodic audits of Text Recruit, its Personnel, and NKPs.
2. Any Personnel or NKPs who violate any provision of this Policy may be subject to disciplinary action, up to and including immediate termination of their employment or contractual relationship (as applicable), as is determined appropriate in management's discretion.
3. In accordance with the Principles, Text Recruit has named the European Data Protection Authorities as the independent recourse mechanism for investigation of an individual's complaints and disputes.

10. DATA BACKUP AND DISASTER RECOVERY

Text Recruit, through its incident response policies and procedures shall notify the subscriber without undue delay when it becomes aware of a Personal Data Breach affecting the subscribers Personal Data.

Additionally, Text Recruit implements an Incident Response Policy and Procedure that ensures a consistent and effective approach to the management of a Security Incident including a Data Breach. Data Breaches usually occur through the unauthorized or accidental use or disclosure of Sensitive and/or Confidential Information by Personnel or by a deliberate attack on the Company's systems.

Security Incidents, including Data Breaches, are handled in accordance with the terms of the agreement between Text Recruit and the subscriber and Text Recruit's Incident Response Procedures.