North America Privacy Policy – Employees (Prospective, Current and Former) (Effective Date: May 25, 2018 (Last Modified May 3, 2024)

I. Introduction.

Your privacy is important. This North America Privacy Policy (the "**North America Privacy Policy**") together with its addendums, the terms and conditions of your Employment Agreement, as amended from time to time (the "**Employment Agreement**"), if any, and any employee handbook or policy, as amended time to time, explains how we deal with applicable privacy requirements and sets out the basis on which our United States entities, Frank Recruitment Group Inc. ("**FRG Inc. USA**") and Frank Recruitment Group Services Inc. ("**FRGS**"), and our Canadian entity, Frank Recruitment Group Inc. / *Groupe de Recrutement Frank Inc.* ("**FRG Canada,**" collectively with FRG Inc. USA and FRGS, "**we**," "**us**," "**our**," or "**FRG**") collect, process, store, use, disclose and remove your personally identifiable information, private information, sensitive information, personal information, or personal data ("**Personal Information**" or "**PII**"). If you apply for a job with FRG, this policy applies to you. Likewise, if you become an FRG employee, this policy applies to you. While employed by FRG, you may work for one or more of our brands - Mason Frank, Nelson Frank, Nigel Frank, Anderson Frank, Jefferson Frank, Washington Frank, FRG Technology Consulting, The Tenth Revolution Group and Revolent Group. Regardless of the brand that you work in at the time, if you are an FRG employee, this policy applies to you.

If you would like a copy of FRG's Information Security Policy Framework, please email FRG's Chief Privacy Officer ("**CPO**") at privacy@tenthrevolution.com.
If you are an EEA, UK or Swiss citizen or resident who FRG employs in the USA or who applied for employment with FRG in the USA, FRG will provide you with a copy of its U.S. Data Privacy Framework HR Privacy Policy & Data Protection Policy, which is incorporated herein by reference. Please see this policy for further information on the processing and protection of your Personal Information in the USA. If you are an EEA, UK or Swiss citizen or resident who FRG employs outside North America, please see the Rest of World Privacy Policy- Employees for further information on the processing and protection of your Personal Information in the USA.

The first part of the notice is general and applies throughout the USA and Canada. The second part of the North America Privacy Policy is comprised of USA state-specific addendums. The third part of this North America Privacy Policy is our Canada Addendum which applies to FRG Canada only. Where applicable, FRG will handle, store, disclose and treat your Personal Information in accordance with then current state, provincial, local, and municipal laws. Please be sure to check the addendums to see if there is one that applies to the state, province, or municipality in which you are working for FRG. In the event of a conflict between the general part of this North America Privacy Policy and an addendum, the addendum prevails.

This North America Privacy Policy applies regardless of the form or method by which you provide Personal Information to FRG. This North America Privacy Policy applies to Personal Information that you provide to FRG in writing, over any website or application operated or used by FRG, FRG's intranet, via email, via text messages (or similar forms of communications), via video conferencing or telephonically.

Please read the following carefully to understand our views and practices regarding your Personal Information, how we will treat it and your rights.

The employee handbook, FRG policies or your Employment Agreement may contain additional terms and obligations related to your use of the internet at work or any FRG equipment, printers, computer systems, Devices (as defined below), computers, databases and email. Please read those documents carefully. In the event of a conflict with respect to data privacy between this North America Privacy Policy, on the one hand, and any FRG policy or employee handbook or your Employment Agreement, on the other hand, the terms of this North America Privacy Policy shall prevail.

FRG's issuance of this North America Privacy Policy does not otherwise change, alter, eliminate or reduce any of your or FRG's obligations under your Employment Agreement or any FRG policy or employee handbook and does not change your "at will" employment status.

II. Who are we?

FRG is a global niche technology recruitment, talent creation, and consulting company that operates under the brands Nigel Frank, Anderson Frank, Mason Frank, Nelson Frank, Jefferson Frank, Washington Frank, FRG Technology Consulting, The Tenth Revolution Group, Revolent Group, and Dynamic Jobs.

The contact details of Frank Recruitment Group's CPO are:

Frank Recruitment Group Services Limited
The St. Nicholas Building
St. Nicholas Street
Newcastle-Upon-Tyne
Tyne & Wear UK NE1 1RF
Attn: Chief Privacy Officer
Email: privacy@tenthrevolution.com

III. Who does this North America Privacy Policy protect?

This North America Privacy Policy applies to all FRG employees based in the USA and Canada, regardless of which FRG affiliate is your actual employer, your title, what brand or team you work on, whether you work in "Support," "Central Services" or "Front Office" at FRG, what office you work in or if FRG employs you remotely. This North America Privacy Policy is inapplicable to FRG employees based outside the USA and Canada for which there is a separate global (excluding USA and Canada) Privacy Policy. If you would like information on FRG's Global (excluding USA and Canada) Employee Privacy Policy, please email privacy@tenthrevolution.com. This North America Privacy Policy applies to Personal Information that you provide to FRG during the employment application process (regardless of whether you actually become an FRG employee), during employment and after employment. If this North America Privacy Policy applies to you, you may be referred to herein as a "**Data Subject**" or collectively, "**Data Subjects**."

This North America Privacy Policy is inapplicable to FRG clients, candidates, independent contractors, freelancers, vendors, partners or suppliers.

IV. What information will we collect?

Some of the data that we collect or receive about you is Personal Information including but not limited to:

- Your name;
- Your gender;
- Your contact details e.g. email address, cell phone number, home phone number, street address;
- Social security number, social insurance number, or other similar number;
- Visa number;
- Passport number;
- Past and present salary information;
- Bonus, stock and other payment information;
- Company car, computer and other company property information;
- Tax related information;
- Identifiable information about you contained in a "consumer report" as defined by the Fair Credit Reporting Act, as amended from time to time, and any similar state, provincial, or local law;
- employment authorization \ citizenship;
- Date of birth;
- Medical or prescription drug information (if you have gave your explicit consent to this data processing);
- Bank account details;
- Performance appraisals, evaluations, ratings, individual development plans, commendation/awards, disciplinary documents, individual competencies, development actions foreseen;
- Current and former job titles, functions, departments, and organizations;
- Next positions planned and development actions foreseen; and
- Other information directly collected from you during the employment relationship.

Other information that we collect or receive from you or about you is not Personal Information, and is not covered by this North America Privacy Policy.

If your provision of Personal Information to FRG is necessary for FRG to hire you (or consider hiring you as an employee), your failure to provide us with accurate Personal Information may result in FRG not being able to process your employment application or offer you employment, continue your employment or terminate your employment.

Mobile Device Management. This paragraph is applicable to FRG Inc. USA and FRG Canada employees only – not applicable to FRGS employees. Where permitted by applicable law and except as set forth in the addendums hereto, in order to monitor and protect other FRG employee's Personal Information, the Personal Information of FRG clients and candidates, and FRG's other confidential information, proprietary information or trade secrets, FRG may install a mobile device management product on any FRG-issued mobile phone, computer, iPad, tablet or any similar device or on any device owned or leased by you from which or on which you have access to FRG confidential information, proprietary information, trade secrets, FRG email or FRG client, candidate or employee information (each a "**Device**"). This mobile device management service may permit FRG to disable or "kill" the Device, to clear or "wipe" the Device, to see FRG related activity and information on your Device and to track the location of the Device. For more information about FRG's Mobile Device Management policies and practices, please see FRG's "Bring Your Own Device" policy which can be found on FRG's internal human resources information system to which you have access.

No Personal Use of FRG Computer, Computer Systems, Etc. – You are not permitted to use FRG's Devices, mobile phones, desk phones, computers, computer systems, networks, internet or applications for personal or non-business use. Please refer to your employee handbook for further information and details. To enforce this policy and audit compliance with this policy, FRG may, without further notice to you, check and monitor your use of FRG computers, computer systems, databases, networks, internet or applications from time to time.

FRG is entitled to restrict the use of FRG email accounts by using filter technologies, including – but not limited to – spam filters and virus scanners. In many cases, the use of such systems requires an automatic analysis of the content of communication.

The use of FRG email accounts is logged and recorded. The following information are recorded:

- Date/time;
- Addresses of sender and recipient (e.g. IP address, email address);
- Volume transferred;
- Email subject, content and attachments.

The information will be used for the purposes of:

- Ensuring the security of FRG's system, analysis and correction of technical errors and malfunctions;
- Determining the scope of use;
- Ensuring compliance with our policies;
- Protecting FRG's intellectual property rights and/or trade and/or business secrets;
- Protecting employees', candidates' and clients' Personal Information.

The information will be stored for as long as legally permitted, unless otherwise required for reasons of data and system security.

As far as possible, the data collection is performed pseudonymously. If FRG's review of the data collected results in evidence of malfunctions, threats, viruses, dangerous content or violations of this North America Privacy Policy, your Employment Agreement , the employee handbook or any FRG policy, FRG is entitled to immediately, and without notice to you, except as where prohibited by applicable law, conduct a complete and thorough review of your use of any Devices and FRG's desk phones, computers, computer systems, databases, networks and applications as well as any logged information, especially with regard to any Personal Information logged and stored in this context. If the review results in a finding of no threats or violations of your Employment Agreement, the North America Privacy Policy, the employee handbook or any FRG policy, or if the data uncovered in the review is no longer needed, FRG will delete the data or have a third party delete the data in accordance with applicable law.

All emails and files sent and received through the FRG's email system are part of FRG's records. In order to comply with legal and contractual retention requirements and other legitimate business purposes, FRG records emails and files sent through its email system. FRG will only keep such records as long as legally permitted or required. If FRG stores any copies of the content for a period of time, FRG may delete such copies from time to time without notice to you, unless such notice is legally required.

Video/CCTV Surveillance. FRG may also engage in limited video/CCTV surveillance as allowed under applicable law. Please see your employee handbook for more information on video/CCTV surveillance. Also note that owners, service providers or lessors of buildings where FRG has offices may use video/CCTV surveillance which are not owned or operated by FRG.

It is possible that your Personal Information may be inadvertently monitored, intercepted, reviewed or erased by FRG while exercising its rights under this section except as prohibited under applicable law.

It is possible that another person's Personal Information may be inadvertently monitored, intercepted, reviewed or erased by FRG while exercising its rights under this policy. If that is the case, FRG will make no use of such other person's Personal Information unless such other person consents to FRG's use of the Personal Information, or the other person's data relates to an actual or potential FRG or government investigation, a legal proceeding involving FRG, a criminal matter, a matter of urgent public or government interest or an emergency.

Use of the Information Obtained from Monitoring and Related Activities. FRG may use the information gathered from its monitoring and related activities of your use of the internet at work, FRG's computers, computer systems, printers, networks, desk phones, phone systems, databases, email systems, applications (such as Skype, Microsoft Teams, Fuze, WhatsApp and instant messenger) and Devices for any action or use allowed by applicable law including, without limitation:

(a) the data or information gathered relates to:
    (i) an actual or potential FRG or government investigation;
    (ii) an actual or potential legal proceeding involving FRG,
    (iii)a criminal matter;
    (iv)a matter of urgent public or government interest; or
    (v) an emergency;
(b) to assist in determining if you or any other FRG employee has violated their contract of employment or any other FRG policy or notice (including this notice), standard or instruction in force from time to time;
(c) to discipline you or any other FRG employee, up to and including dismissal;
(d) to assist in determining if any supplier, contractor, candidate or client has violated FRG's contractual or other rights;
(e) to protect FRG's intellectual privacy rights, company data or trade secrets;
(f) to enhance FRG's compliance with applicable law or stop any potential violation of law by FRG or any other person or entity;
(g) to prevent misuse of FRG computers, computer systems, phone, phone system, networks, databases, email accounts and the Device that could harm FRG;
(h) to ensure compliance with our rules, standards of conduct and policies in force from time to time (including this North America Privacy Policy);
(i) to monitor your or other FRG employees' performance at work and your compliance with your Employment Agreement;
(j) to ensure that FRG business matters are responded to and progressing such as supplier, candidate and client matters while you are out of the office for any reason or no longer employed by FRG;
(k) to inspect and identify if any FRG, client or candidate confidential information or Personal Information is stored on any FRG printer, desk phone, phone system, network, database, email system or application (such as Skype, What's App, Microsoft Teams, Fuze or instant messenger) or Device;

(l) to investigate or resolve any security incident or unauthorized use of the internet at work, any FRG printer, desk phone, phone system, network, database, email system, application (such as Skype, What's App, Fuze, Microsoft Teams and instant messenger) or Device;
(m) to ensure that employees do not use any FRG printer, desk phone, phone system, database, network, phone, phone system, email system, application (such as Skype, What's App, Fuze, Microsoft Teams and instant messenger) or Device for any unlawful purposes or activities that may damage our business or reputation; and
(n) FRG's email systems or accounts for personal use.

Without limiting any other right or remedy of FRG, if we discover or reasonably suspect that any of the above listed events is occurring or may imminently occur, we may immediately remove your or your Device's access to our systems, networks, databases and environments. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or emails), it may not be possible to distinguish all such information from FRG, client or candidate data in all circumstances. You should therefore regularly backup any personal data contained on any Device.

Do Not Track. If FRG receives a "Do Not Track" signal or request from a web browser, FRG will not honor such request or signal. FRG has taken this position in part to provide you with a personalized and efficient experience on the Websites.

V. Why do we process your Personal Information?

FRG will store, process and use your Personal Information to conduct its business and comply with applicable local law, including in some or all of the following ways:

- To facilitate the hiring and interview process;
- To facilitate the compensation and wage payment process or to correct any issue with your compensation or payment;
- To complete and submit documents required by government agencies or applicable law;
- To provide health, dental and other benefits to you or a family member;
- To pay you pension, national/social insurance, medical or other payments to you or on your behalf;
- To provide you with retirement benefits, where applicable (like 401(k)s or pension plans);
- To provide you with information necessary for your taxes;
- To investigate, respond to or resolve any employment related compliant or issue made by, about or involving you,
- To investigate and respond to any leave of absence you may request,
- To terminate your employment or to consummate your resignation of employment with us;
- To provide you with a service requested by you, like verifying your employment or compensation for a loan or a mortgage;
- To extent permitted by applicable law, to monitor or ensure your appropriate use of the phone and internet at work and any FRG computers, computer systems, printers, phone, phone system, networks, databases, email systems, applications (such as Skype, What's App, Microsoft Teams, Fuze and instant messenger) and Devices;
- To extent permitted by applicable law, to monitor your compliance with your obligations under your Employment Agreement, any FRG policy or our employee handbook;
- To make it possible for you to travel on FRG business or on an award or incentive trip;
- To enable you to submit your resume to FRG for employment, to apply online including through any website or online application operated by FRG (collectively, the "**Websites**"));

- To answer your questions and enquiries;
- To use your information on an anonymized or pseudonymized basis to monitor compliance with our equal opportunities policy, other FRG policies and any legal or compliance requirements;
- To carry out our obligations arising from any contracts entered into between you and us, including your Employment Agreement;
- To enforce any of your contractual obligations to us, including those under your Employment Agreement, in an FRG policy on in our employee handbook;
- To fill an open vacancy at FRG and to advise you of vacancies at FRG for which FRG believes you may be qualified or interested in;
- To input your Personal Information into FRG's applicant or human resources database;
- To qualify or screen you to determine if you are qualified for an FRG vacancy;
- To work with you through the interviewing process;
- To answer any questions you may have regarding an FRG job vacancy;
- To draft, negotiate, change or enforce your Employment Agreement and to draft, revise, negotiate or answer any questions you may have about your Employment Agreement, any FRG policy or our employee handbook;
- To complete your onboarding process (including any necessary or required background checks);
- To facilitate and complete your off boarding process;
- To offer you, enroll you in or answer questions you may have about any benefit of employment;
- To change any election you have made regarding your employment or any employee benefits;
- To process any changes to any term or condition of your employment;
- To answer any questions from your representative, executor, accountant, attorney, spouse or child (after obtaining any required consent from you where legally required and feasible) related to your employment;
- To cooperate with any government agency in any audit, inquiry or investigation or any governmental requirement;
- To complete and file any employment related tax returns and to pay any employment related taxes or other deductions;
- To reclaim or receive any amounts owed by you to us;
- In connection with and to improve FRG's diversity and inclusion programs and policies;
- If you are a job applicant, to send you electronically or by post communications regarding the job application process; and
- To exercise or defend any legal claims against you, made by you or involving you.

VI. Who do we share your Personal Information with?

We may share your Personal Information with third parties in connection with your employment or potential employment at FRG. Some of the most common examples of this are:

- With insurance or benefits brokers, vendors, "umbrella" companies, carriers or providers;
- With retirement benefit brokers, vendors, trustees or providers;
- With third parties who you request;
- With payroll vendors and providers;
- With government agencies in connection with any visa or similar issue or proceeding;
- With background check and employment and education verification providers;
- With drug screening companies;
- With non-benefit insurance brokers or carriers in connection with any claim under a policy of insurance maintained by FRG;

- With consultants or software providers who build, maintain or develop computer systems for FRG such as the HR database;
- With mobile phone providers if we are issuing you a mobile phone;
- With third parties to provide data storage services;
- With third parties who provide the mobile device management service described above;
- With third parties in connection with assisting FRG in its diversity and inclusion programs and policies;
- To third parties, regulatory or law enforcement agencies if we believe in good faith that we are required by law to disclose it in connection with the detection of crime, the collection of taxes or duties, in order to comply with any applicable law or order of a court of competent jurisdiction, or in connection with legal proceedings;
- To third parties to determine if an FRG competitor, client, or other entity (or their respective affiliates) has (a) employed you or (b) retained you or any entity (i) that employed you or (ii) that retained you or (iii) in which you have an financial interest.
-
- To FRG affiliates, whose locations can be found at https://www.frankgroup.com/contact. These entities will process your Personal Information in accordance with this North America Privacy Policy; and
- In the event of a sale, merger, liquidation, receivership or transfer of all or substantially all of the assets, or a controlling interest in the equity, of FRG (or any of its group companies) provided that such counterparty(ies) to any such transaction agrees to adhere to the terms of this North America Privacy Policy (or a similar document).

The third parties referenced above have agreed to maintain the confidentiality of, and to protect, your Personal Information in accordance with applicable law.

VII. What will FRG do if my Personal Information is breached?

FRG has put in place reasonable technical, administrative and physical safeguards intended to prevent a breach of your Personal Information. That being said, FRG cannot guarantee that your Personal Information will not be breached.

A breach can take many forms, including, without limitation, the loss of your Personal Information or the unauthorized access to, disclosure, modification, copying and transfer of your Personal Information. Once FRG becomes aware of the breach, FRG will take reasonable steps to isolate the breach, stop the breach, determine the root cause, determine the Personal Information breached, fix the root cause and determine if notice to you and/or the appropriate government agency(ies) is required. FRG will comply with all applicable law in reacting to, and dealing with, a breach of Personal Information.

If you believe, for any reason, that your Personal Information has been breached while in FRG's care, custody or control, please email FRG immediately at privacy@tenthrevolution.com.

VIII. Will my Personal Information be transferred to another country?

Yes, FRG may transfer your Personal Information to the categories of third parties described in this North America Privacy Policy, some of whom are located outside of the country in which you provided your Personal Information to FRG or the country of collection.

If so, FRG will take reasonable steps to ensure that your Personal Information is protected and treated in accordance with this North America Privacy Policy and local applicable law. The countries where FRG may transfer your Personal Information will have varying levels of data security practices and laws, some of which may be less stringent or protective than your country. FRG will use all reasonable efforts to require that any of its suppliers and vendors who receive your Personal Information are contractually bound to (a) keep your Personal Information confidential and (b) take, at a minimum, all reasonable efforts to maintain the privacy and security of your Personal Information.

Under certain circumstances, FRG may share your Personal Information with one or more of its group companies who may be located outside of the USA or Canada. In such cases, FRG will comply with applicable laws and its Intercompany Data Processing Agreements ("DPAs"). The DPAs are incorporated by reference into this North America Privacy Policy.

IX. How long will FRG store my Personal Information for?

We are required by law to store your Personal Information for the identified purposes as long as is necessary to comply with our statutory and contractual obligations which in most cases will extend beyond the cessation, for any reason, of your employment with FRG or, if you never became an employee of FRG, the termination of your employment application process.

Furthermore, we will store your Personal Information post-employment or employment application process so that FRG can issue or respond to any claims arising out of your employment or prospective employment with FRG, or in connection with any investigation by or of a government authority related to your employment or prospective employment with FRG.

X. Sending Personal Information over the internet

Your Personal Information is held on servers hosted by us, our internet services providers or third party vendors with whom FRG has a contract. The transmission of information via the internet is not completely secure. Although we will take the efforts set forth in the North America Privacy Policy to protect your Personal Information, we cannot guarantee the security of any data transmitted through or to our Websites or any network or computer system. Any transmission of data by you to us over the internet is at your own risk.

XI. Changes to our North America Privacy Policy

We reserve the right to change this North America Privacy Policy from time to time by updating our intranet site or internal human resources portal or website. Any changes to this North America Privacy Policy will be posted on our intranet and may be communicated to you via email so you are always aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. We encourage you to check the intranet frequently for updates. Your employment, continued employment or engagement in the employment screening process constitutes your acceptance of the revised North America Privacy Policy.

FRG will interpret and enforce this North America Privacy Policy in accordance with all applicable law.

This North America Privacy Policy, formerly known as a "Privacy Notice," and "US Privacy Policy," was first issued on May 25, 2018.

FRG updated and amended this North America Privacy Policy, formerly known as a “Privacy Notice,” and “US Privacy Policy,” on October 8, 2018, September 8, 2020, July 29 ,2021, and December 2022.

FRG last updated and amended this North America Privacy Policy March 4, 2024.

Employee Certification

By signing below, I certify that I have read and understand Frank Recruitment Group's North America Privacy Policy – Employees, and consent to its terms.

_____	_____	_____
Printed Name	Signature	Date

CALIFORNIA CCPA/CPRA ADDENDUM

We prepared this CCPA/CPRA Addendum ("**CCPA/CPRA Addendum**") to help you understand our practices regarding the collection, use, and disclosure of information we collect from you through FRG's web applications, our websites that link to this CCPA/CPRA Addendum, and any other services we provide to our employees/customers (collectively, "Services"). By accessing or using the Services, you agree to this CCPA/CPRA Addendum, in addition to any other agreements and policies you have agreed to through FRG and/or your Employment Agreement.

The California Consumer Privacy Act ("**CCPA/CPRA**") requires businesses subject to the law to provide consumers residing in California ("**consumer**" or "**consumers**") with the right to opt out of the sale or sharing of their personal information through a clear and conspicuous link on their main homepage called "Do Not Sell My Personal Information." Under some circumstances, Employees who are California residents are consumers under the CCPA/CPRA.

If a business maintains a separate webpage dedicated to California consumers rights, it can put the Do Not Sell link on that page instead of on its main homepage as long as it takes reasonable steps to direct California consumers to that page.

The California Attorney General may also develop a "recognizable and uniform opt-out logo or button" for all businesses to promote consumer awareness of the right to opt out. If the AG develops this, businesses should use it instead of a text link.

Businesses may not require a consumer to create an account in order to opt out of sales or sharing of personal information, and they may only use the information collected during the opt-out to comply with the opt-out.

When a consumer opts out, businesses must not sell or share their personal information and cannot ask them to opt-in again for 12 months from the date of opt out.

Does FRG need to train its employees and vendors about the CCPA/CPRA?

Yes. Businesses also need to train their staff who handle consumer requests about privacy, including making sure they:

- Know about the CCPA/CPRA generally
- Can inform consumers about how to exercise their rights
- Understand how to access the "Do Not Sell My Personal Information" page and how it works
- Do not sell or share the personal information of consumers who opt out (or who have not opted in, in the case of children aged 16 or younger)
- Wait 12 months before asking consumers who opted out to opt in again
- Use any personal information collected as part of an opt out only to process the opt out
- Respect opt outs made by an authorized agent on behalf of another person if such authorized agent provides signed written permission from the other person to do so.

Information from Children

FRG is not directed to children under the age of 13 and we do not knowingly collect personally identifiable information from children under the age of 13. If we learn that we have collected personally identifiable information of a child under the age 13, we will take reasonable steps to delete such information from our files as soon as is practicable. You are required to contact the Privacy Team at privacy@tenthrevolution.com, fill the webform below, or give us a call at 1-866-I-OPT-OUT (1-866-467-8688) and enter Service Code 717 if you believe we have any information from or about a child under the age of 13.

California Consumer Privacy Act Disclosures

The California Consumer Privacy Act, or CCPA/CPRA, requires businesses subject to this law to provide consumers residing in California with certain rights regarding their personal information and sensitive personal information.

At this time, we may sell or share your personal information and depending on the circumstances, your sensitive personal information, so the opt-out or opt-in choices may apply. For more information, visit www.frankgroup.com/donotsell.

Here's a summary of rights for California consumers under the CCPA/CPRA:

I. Your Right to Opt Out. You have the right to tell businesses that do sell or share your personal information as well as sensitive personal information to third parties (i.e. not us) not to sell or share it at any time. Businesses that sell or share your personal information or sensitive personal information to third parties must also ensure that the third parties do not resell or share it unless the business notified you explicitly and provided you with a chance to opt out of resales or shareing. These opt-out rights apply to businesses that do not know your age, or know you are older than 16. Additionally, we must also respect opt outs made by your authorized agent if such authorized agent provides signed written permission from you to do so.

II. Your Right to Opt In. If a business has actual knowledge that you are between ages 13 and 16 (e.g., based information the business collects), businesses cannot sell or allow resales or sharing of your personal information or sensitive personal information without your affirmative authorization. If a business has actual knowledge that you are younger than 13, it may not sell or share or allow resales or reshares of your personal information or sensitive personal information without your parent or guardian's affirmative authorization. This is your right to opt in.

III. Your Right to Disclosures. You have the right to know:

1. A link to FRG's "Do Not Sell My Personal Information" notice.
a) Please visit frankgroup.com/donotsell.

2. A description of a consumer's rights pursuant to CCPA/CPRA Section 1798.120:
a) Your Right to Opt Out. If you're a consumer residing in California and we sell your information to third parties, you can tell us at any time not to sell or share your personal information or sensitive personal information. This right to opt-out applies if we do not know your age or if we know you are older than age 16.

b) Your Right to Opt In. If we have actual knowledge that you are between ages 13 and 16 (e.g., based information we collect, or because someone informed us), we will never sell or share your personal information or sensitive personal information without your affirmative authorization. If we have actual knowledge that you are younger than 13, we will never sell or share your personal information or sensitive personal information without your parent or guardian's affirmative authorization. This is your right to opt in.

c) Do We Sell Or Share Your Personal Information or Sensitive Personal Information? At this time, we may sell or share your personal information and/or sensitive personal information and you can opt out at any time. If you opt out, or for children 16 and younger, if you have not opted in, we will not sell your personal information or sensitive personal information to third parties unless you expressly authorize us to do so.

3. A description of a consumer's rights pursuant to CCPA/CPRA Section 1798.110: California consumers have the right to request that we disclose to you:

a) The categories of personal information it has collected about you.

b) Personal information is information that identifies or relates to a particular consumer or household including name; postal address; email address; IP address; social security number; personal property records; purchasing histories; biometric information; internet activity such as browsing or search history, geolocation data, audio, electronic, visual, thermal, olfactory, or similar information; employment information; sensitive personal information; education information and inferences drawn from this information; in so far as the above are not publicly available information. In addition to the above types of personal information that we may collect, FRG may also collect the following types of personal information:

i) Name;

ii) Contact details e.g. street address, email address, telephone number;

iii) Work Experience;

iv) Job Title;

v) Professional Certifications;

vi) Education & Qualifications;

vii) Skills;

viii) Career History;

ix) Salary Range;

x) Right to work status \ citizenship;

xi) Other information relevant to help us provide recruitment and talent creation services;

xii) References from past employers; and

xiii) IP address

c) "Sensitive personal information" means: nonpublic personal information that reveals:

i) A consumer's social security, driver's license, state identification card, or passport number;

ii) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;

iii) A consumer's precise geolocation;

iv) A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;

v) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication;

vi) A consumer's genetic data;

vii) The processing of biometric information for the purpose of uniquely identifying a consumer;

viii) Personal information collected and analyzed concerning a consumer's health; and

ix) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation

4. The categories of third parties with whom the business shares personal information and/or sensitive personal information.
a) All users of the websites and/or our services

i) To third parties where we have retained them to provide services that we or you have requested or that FRG clients have requested including references, qualifications and background reference checking services and to verify the details you have provided from third party sources.

ii) To third parties to provide data storage, resume parsing, data cleansing and marketing (via email & SMS, standard SMS and text rates may apply) services to FRG where such third parties have agreed to maintain the confidentiality of, and to protect, your personal information in accordance with applicable law.

iii) To third parties to assist with credit control and payment management.

iv) To third parties, regulatory or law enforcement agencies if we believe in good faith that we are required by law to disclose it in connection with the detection of crime, the collection of taxes or duties, in order to comply with any applicable law or order of a court of competent jurisdiction, in connection with legal proceedings or other similar cause or circumstance.

v) To FRG affiliates, whose locations can be found at https://www.frankgroup.com/contact. These entities will process your personal information in accordance with the CCPA/CPRA Addendum.

vi) In the event of a sale, merger, liquidation, receivership or transfer of all or substantially all of the assets, or a controlling interest in the equity, of FRG (or any of its group companies) provided that such counterparty(ies) to any such transaction agrees to adhere to the terms of the CCPA/CPRA Addendum (or a similar document) and applicable law.

b) Actual or Prospective Candidates
i) To FRG clients in order for them to determine if you (permanent hire candidate) or your company or employer (contract candidate) are or may be qualified to fill a vacancy.

ii) •To third parties that you authorize us to send your personal information to such as "umbrella companies," insurance brokers, and insurance carriers.

iii) To third parties to determine if an FRG client or other entity (or their respective affiliates) to whom FRG presented you has (a) employed you or (b) retained you or any entity (i) that employed you or (ii) that retained you or (iii) in which you have an financial interest.

c) Individuals who work for FRG clients (i.e. a client contact)
i) To candidates in the course of providing your company or employer with recruiting services and to further the recruitment or talent creation process.

ii) To third parties where we have retained them to provide services that you have requested including candidate skill tests and other testing.

iii) To third parties to determine if an FRG client or other entity (or their respective affiliates) to whom FRG presented a candidate has (a) employed the candidate or (b) retained the candidate or any entity (i) that employed the candidate or (ii) that retained the candidate or (iii) in which the candidate has a financial interest.

5. The categories of sources from which the personal information and/or sensitive personal information is collected.

a) We collect personal information and/or sensitive personal information from you actively when you enter it into our services (e.g., your name, your resume, etc., your Employment Agreement, onboarding information, your bank accounting information (for deposit information), emergency contacts/next of kin information, a copy of your passport/visa information (if applicable), HR profile, information entered into HIVE, etc.).

b) We collect personal information and/or sensitive personal information passively when you access our services, to the extent your web browser provides this information to our servers (e.g., your operating system) and also based on your service usage (e.g., when and from what IP address you log on to our services).

c) We collect personal information and/or sensitive personal information when it is provided to us by either yourself or a third party (for example, LinkedIn, Job board, resume databases, etc.).

6. The business or commercial purpose for collecting, selling, or sharing personal information and/or sensitive personal information.

a) Why do we process your personal information?

i) Generally, we use your personal information and/or sensitive personal information for our business and activities (including facilitating your employment with us), and in our efforts to expand and improve our business. Examples include but are not limited to the following:

1. All users of the Websites and/or our services

a) to provide our recruitment and talent creation services to you, your employer or your company (applicable to users of our websites who are not employees);

b) To facilitate the recruitment and talent creation process, including but not limited to:

i) Qualifying and submitting candidates;

ii) For clients, negotiating FRG terms of business;

iii) Arranging interviews and obtaining feedback;

iv) Negotiating compensation packages; and

v) Providing post placement follow up.

c) To assess data about non-employees against vacancies which we judge may be suitable for those non-employees;

d) To third party vendors to assist us in hosting, managing and operating our websites;

e) To third party vendors who provide data analysis and data updating services to us;

f) To third party vendors who provide email and other communications related services to us

g) To enable non-employees to submit their resume to FRG, apply online (including through the Websites) for jobs or to subscribe to alerts about jobs we think may be of interest to those non-employees;

h) To enable us to develop and market other products and services and where you have consented to being contacted for such purposes;

i) To improve our customer service and to make our services more valuable to you (including tailoring the Websites when you log on to enrich your personal online experience);

j) To send you electronically or by post surveys, reports, FRG event details, promotions, offers, networking and client events and general information about relevant industry sectors which we think might be of interest to you, where you have consented to being contacted for such purposes (and we will provide you with an opportunity to opt out);

k) To identify you, and respond to and process your requests for information and provide you with a product or service;

l) To amend records to remove personal information;

m) To use your information on an anonymized basis to monitor compliance with our equal opportunities policy, other FRG policies and any legal or compliance requirements;

n) To use your information on an anonymized basis to create marketing materials such as a salary survey; and

o) To carry out our obligations arising from any contracts entered into between you and us, and for other everyday business purposes that involve use of personal information.

2. Actual or Prospective Candidates
a) To help find you or your company a job;

b) To contact you (permanent hire candidates), your employer or your company (contract candidates) about jobs that FRG is filling or may fill for FRG clients;

c) To provide you or your company with information about the job market;

d) To communicate with you (permanent hire candidates), your employer or your company (contract candidates) after you or it has started a job to make sure all is going well or to remedy, or attempt to remedy, any problems;

e) To answer any questions you have about a job or the job market;

f) To fulfill any aspect of your employer's or your company's contract with FRG (for contract candidates only);

g)To third party vendors who provide customer relationship management database services to us;

h) To third party vendors who provide data analysis and data updating services to us

i) To third party vendors who provide document execution, transmission and storage services to us

j) To third party vendors who provide email and other communications related services to us

k) To collect any money due, or allegedly due, to FRG or any FRG client (or FRG's client's client);

l) To obtain or inquire about any property (including computers and confidential business information) owned, or allegedly owned, by FRG or any FRG client (or FRG's client's client);

m) To establish, exercise or defend any legal claims; and

n) To assist you (permanent hire candidates), your employer or your company (contract candidates) if you are dissatisfied or dislike the job, or any aspect of it.

3. Individuals who work for FRG clients (i.e. a "client contact")
a) To fill an open vacancy at your company or employer;

b) To contact you about candidates for jobs with whom FRG has a relationship;

c) To provide you with information about the job market;

d) To third party vendors who provide customer relationship management database services to us;

e) To third party vendors who provide data analysis and data updating services to us

f) To third party vendors who provide document execution, transmission and storage services to us

g) To third party vendors who provide email and other communications related services to us

h) To communicate with you after your company or employer has hired/retained an FRG candidate to make sure all is going well and to remedy, or attempt to remedy, any problems;

i) To negotiate and fulfil any aspect of your company's or employer's contract with FRG;

j) To answer any questions you have about a job or a candidate or your company's or employer's contract with FRG;
k) To resolve any issue with the issuance, payment, collection or enforcement of an FRG invoice;

l) To collect any property owned by FRG or any FRG candidate;

m) To establish, exercise or defend any legal claims.

7. The specific pieces of personal information and/or sensitive personal information it has collected about that consumer.
a) Please email us at privacy@tenthrevolution.com, fill out the webform located at: https://www.frankgroup.com/privacy-notice/#ccpaform**,** or call us toll free at 1-866-I-OPT-OUT (1-866-467-8688) and enter Service Code 717 to request this information. Before we can respond to your request, we'll need to verify your identity.

8. A description of a consumer's rights pursuant to CCPA/CPRA Section 1798.115:
a) If we sell your personal information and/or sensitive personal information or disclose it for a business purpose, you have the right to know:

i) The categories of personal information and/or sensitive personal information that the business collected about the consumer.
1) See Section 3 d) above (e.g., web log data, registration data, resume data, etc.).

ii) The categories of personal information and/or sensitive personal information that the business sold or shared about the consumer and the categories of third parties to whom the personal information and/or sensitive personal information was sold or shared, by category or categories of personal information and/or sensitive personal information for each third party to whom the personal information and/or sensitive personal information was sold or shared.
1) See Sections 3 d), 3 e), 3 f), and 3 g) above.

iii) The categories of personal information and/or sensitive personal information that the business disclosed or shared about the consumer for a business purpose.
1) See Section 3 f) above.

b) If we sell or share your personal information and/or sensitive personal information or disclose it for a business purpose, you have the right to request that we disclose to you (1) the categories of personal information and/or sensitive personal information that we collected about you, (2) the categories of personal information and/or sensitive personal information we sold or shared about you and the categories of third parties to whom we sold or shared it, by category of personal information for each third party to whom we sold or shared your personal information and/or sensitive personal information and (3) the categories of personal information and/or sensitive personal information that the business disclosed about the consumer for a business purpose. We are required to verify your identity before providing you with this information if the information would constitute your personal information. To exercise these important rights, please: mail us at privacy@tenthrevolution.com, fill out the webform located at: https://www.frankgroup.com/privacy-notice/#ccpaform, or call us toll free at 1-866-I-OPT-OUT (1-866-467-8688) and enter Service Code 717 to request this information. Before we can respond to your request, we'll need to verify your identity.

c) If we sell or share your personal information and/or sensitive personal information to a third party or disclose it for a business purpose, we are required to disclose:

i) The category or categories of consumers' personal information and/or sensitive personal information we sold or shared, or if we have not sold or shared your personal information and/or sensitive personal information, we shall disclose that fact.
1) If we sell or share your personal information and/or sensitive personal information, it will be in the form of your resume, anonymized or pseudonymized.

ii) The category or categories of consumers' personal information and/or sensitive personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information and/or sensitive personal information for a business purpose, it shall disclose that fact.
1) We rely on vendors to operate our infrastructure, and accordingly for each category of personal information and/or sensitive personal information that we disclosed above as a category that we collect, we disclose it to one of our third-party vendors for a business purpose (i.e. to develop, market, provide and support our business services). Those categories are: web log data, registration data, payment data, service usage data, customer content, consumer content and marketing data.

d) If we sell or share your personal information and/or sensitive personal information to a third party, it is not allowed to resell or reshare it unless we notified you explicitly and provided you with a chance to opt out.

1) We do not allow third parties to whom we sell or share your personal information and/or sensitive personal information to resell or reshare the personal information and/or sensitive personal information, so no opt-out choices apply. See https://www.frankgroup.com/privacy-notice/#ccpa for details.

9. A description of a consumer's rights pursuant to CCPA/CPRA Section 1798.125:

a) Businesses, including us, may not discriminate against you because you exercised any of your consumer privacy rights such as by: (1) denying you goods or services; (2) charging you different prices or rates for goods or services, including via discounts or other benefits or penalties; (3) providing you a different level or quality of goods or services or (4) suggesting that you will receive a different price or rate for goods or services or a different level or quality of goods or services. Businesses may however discriminate where any difference is reasonably related to the value provided to you by your data.

b) Businesses, including us, may offer you financial incentives, including payments as compensation, for the collection, sale or deletion of your personal information and/or sensitive personal information. If we offer any incentives we will (1) notify you about them in our privacy policy and in any California-specific descriptions of consumer privacy rights we post and (2) only enroll you in them with you opt-in consent after disclosing all material incentive program terms to you. Incentive programs may never be unjust, unreasonable, coercive, or usurious.
i) We do not currently offer any financial incentives.

10. A description of a consumer's rights pursuant to CCPA/CPRA Section 1798.105:
a) You have the right to request that we delete any personal information and/or sensitive personal information about you that we have collected. Before we delete any information, we'll need to verify your identity. If we delete your information, we'll also instruct our vendors (aka service providers) to delete it. The CCPA/CPRA does not obligate us to delete information under all circumstances, including where we need the information to provide our services to you, to detect security incidents, to identify errors in our services, or to comply with legal obligations. If you request that we delete information, we'll let you know if we are deleting it or if we are not deleting it based on exemptions provided by the CCPA/CPRA.

11. One or more designated methods for submitting requests (at minimum, a toll-free telephone number):
a) You may submit any consumer privacy requests, including any respecting sensitive personal information, by emailing us at privacy@tenthrevolution.com, fill out the webform located at https://www.frankgroup.com/privacy-notice/#ccpaform, or by calling us toll free at 1-866-I-OPT-OUT (1-866-467-8688) and entering Service Code 717. Before we can respond to your request, we'll need to verify your identity.

12. A list naming all third parties that FRG allows to collect personal information and/or sensitive personal information from the consumer:

Client-managed Qlik Sense Enterprise	Texty (Salesforce)	Broadbean
AWS	Sage X3	Daxtra
BaseCamp	WordPress	Docomotion
Fuze	Isotoma (Brand/ Brochure websites)	8x8 (telephony)
Hive	Team Viewer	Docusign Gen
HSBC MiVision	Azure	Mimecast
Drift	Concur	Palo Alto
Pardot	Meraki	Sidetrade
6Sense	Microsoft 365 (OneDrive, Sharepoint, OneNote, Teams, Exchange)	Ampps
Atlassian	Netskope	Git Bash
Botstar	SendGrid	Google Analytics
Cisco	Vanguard Retirement (Payroll pension provider)	Google Tag Manager
Dell Switches	Acora	Payworks (Canada Payroll)
DWH	Apollo (Salesforce Revolent)	Reactful

employee navigator (Health insurance + benefits)	winMTR
BRI (commuter benefit plan)	Windows Powershell
DSMN8	SQL Server
HeidiSQL	Windows Snipping Tool
Qualtrics	WinMerge
GitKraken	Atlassian
ZaapIT	Jenkins
Zoominfo	KeePass
Solarwinds	Avalara
HotJar	Hopin
PaperCut	Stripe
Putty	
WinSCP	

IV. Your Right to Data Deletion. You have the right to request that we delete any personal information and/or sensitive personal information about you that we have collected. Before we delete any information, we'll need to verify your identity. If we delete your information, we'll also instruct our vendors (aka service providers) to delete it. The CCPA/CPRA does not obligate us to delete information under all circumstances, including where we need the information to provide our services to you, to detect security incidents, to identify errors in our services, or to comply with legal obligations. If you request that we delete information, we'll let you know if we are deleting it or if we are not deleting it based on exemptions provided by the CCPA/CPRA. You may also delete personal information by using our services dashboard as described above.

V. Your Anti-Discrimination Rights. Businesses may not discriminate against you exercising any of your consumer privacy rights such as by: (1) denying you goods or services; (2) charging you different prices or rates for goods or services, including via discounts or other benefits or penalties; (3) providing you a different level or quality of goods or services or (4) suggesting that you will receive a different price or rate for goods or services or a different level or quality of goods or services. Businesses may however discriminate where any difference is reasonably related to the value provided to you by your data. We will not discriminate against you in any way for exercising your privacy rights.

VI. Your Rights Regarding Financial Incentives. Businesses may offer you financial incentives, including payments as compensation for the collection, sale or deletion of your personal information and/or sensitive personal information. In this case a business must: (1) notify you about the incentives in its CCPA/CPRA Addendum and in any California-specific descriptions of consumer privacy rights it posts and (2) only enroll you in them only with your opt-in consent after disclosing all material incentive program terms. Incentive programs may never be unjust, unreasonable, coercive, or usurious. We do not currently offer any financial incentives.

VII. Designated methods for submitting requests. We offer three ways to express your privacy preferences: the interactive web form located: https://www.frankgroup.com/privacy-notice/#ccpaform, our email at privacy@tenthrevolution.com, or by giving us a call at 1-866-I-OPT-OUT (1-866-467-8688) and enter Service Code 717.

Changes to CCPA/CPRA Addendum

Any information that we collect is subject to the CCPA/CPRA Addendum in effect at the time such information is collected. We may, however, revise the CCPA/CPRA Addendum from time to time. If a revision is material, as determined solely by us, we will notify you, for example via email. The current version will always be posted to our CCPA/CPRA Addendum.

If you have any questions about this CCPA/CPRA Addendum, or wish to exercise any of your privacy rights, please contact us at privacy@tenthrevolution.com or at any of the methods described above.

CANADA ADDENDUM

I. Introduction

This Canada Addendum ("**Canada Addendum**"), in addition to the forgoing North American Privacy Policy, sets out the basis on which all "Personal Information," as defined above, that Frank Recruitment Group Inc. / Group de Recrutement Frank Inc. and its affiliated entities and their respective representatives trading under the following brand names: Nigel Frank, Anderson Frank, Mason Frank, Nelson Frank, Jefferson Frank, Washington Frank, FRG Technology Consulting, The Tenth Revolution Group, Revolent Group, and Dynamic Jobs (collectively for the purposes of this Canada Addendum, "**FRG**," "**we**," "**our**," or "**us**") collects from you, or that you provide to us via the Websites (as defined elsewhere in the North America Privacy Policy) will be processed by us in Canada. If there is a conflict between the North America Privacy Policy and this Canada Addendum, the Canada Addendum controls with respect to Canadian users of our Websites. Please read the following carefully to understand our views and practices regarding your Personal Information in Canada and how we will treat it. All capitalized/defined terms not defined herein are defined elsewhere in the North America Privacy Policy.

II. Canadian Privacy Law and Privacy Principles

FRG is committed to maintaining the confidentiality, security, and accuracy of your Personal Information in accordance with applicable Canadian federal and provincial law, including but not limited to the Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), Canada's Anti-Spam Legislation, SC 2010 c 23 ("**CASL**"), and the data privacy laws of Canada's provincial counterparts including but not limited to the British Columbia Personal Information Protection Act, SBC 2003 c 63 ("**BC PIPA**"), British Columbia Privacy Act, RSBC 1996 c 373 ("**BC PA**"), Alberta Personal Information Protection Act, SA 2003 c P-6.5 ("**AB PIPA**"), Quebec Act respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1 ("**Quebec Private Sector Act**"), An Act to Establish a Legal Framework for Information Technology in Quebec, CQLR c C-1.1 ("**AELFIT**"), Sections 35 and 36 of the Civil Code of Québec, CQLR c CCQ-1991 ("**Quebec Civil Code**"), the Quebec Charter of Human Rights and Freedoms, CQLR c C-12 ("**QCHRF**"), the Manitoba Personal Information Protection and Identity Theft Prevention Act 2013 ("**PIPITPA**"), and the Manitoba Privacy Act, CCSM c P125 ("**MPA**") (collectively, PIPEDA, CASL, BC PIPA, BC PA, AB PIPA, the Quebec Private Sector Act, AELFIT, Quebec Civil Code, QCHRF, PIPITPA, MPA, and other applicable Canadian federal and provincial data privacy, data protection, security, and cyber laws are the "**Canadian Privacy Laws**") to govern our activities as they relate to the use of your Personal Information. As part of this commitment, we follow the ten privacy principles established under the Canadian Privacy Laws which incorporate the legal requirements of the provinces we operate in as well as those established under PIPEDA. These principles (collectively, the "**Canadian Privacy Principles**") are as follows:

- **Principle One: Accountability**
  FRG is responsible for the Personal Information it controls. FRG has designated its Chief Privacy Officer (privacy@tenthrevolution.com (for Revols: privacy@revolentgroup.com)) as responsible and accountable for compliance with the Canadian Privacy Principles and other applicable Canadian Privacy Laws, including for prospective and current employees.

- **Principle Two: Identifying Purpose**
  FRG must identify the purposes for which Personal Information is used, collected, and disclosed before or at the time we collect Personal Information. FRG demonstrates its compliance by making the North America Privacy Policy and this Canada Addendum available to individuals, among other actions.

- **Principle Three: Consent**
  Your knowledge and consent are required for the collection, use or disclosure of your Personal Information, except where inappropriate or permitted by Canadian law. Further, in Quebec, your manifest, free, enlightened, and specific consent is required when collecting Personal Information about you from third parties. Where applicable in Canada, if your consent is necessary for FRG to carry out employee monitoring (including but not limited to electronic monitoring or phone call monitoring), FRG shall obtain your consent as provided below. Depending on the level of sensitivity of the Personal Information, this consent may be implied or

expressed; however, wherever commercially feasible or legally required (for example in Quebec), FRG shall attempt to obtain express consent (and shall, if legally required). By applying for a position with FRG, or by your continued employment with FRG, you hereby manifestly, freely, enlightenedly, and specifically explicitly consent to the use of your Personal Information to the highest extent permitted by applicable law, including the Canadian Privacy Laws and for employee monitoring as described above. Consent to our use of your Personal Information can be withdrawn at any time by sending an email requesting same to privacy@tenthrevolution.com (for Revols: privacy@revolentgroup.com).

- **Principle Four: Limited Collection**
  FRG must collect Personal Information by fair and lawful means and limit its collection of Personal Information to those details reasonably necessary for the purposes identified. Accordingly, except to the extent necessary as permitted by the Canadian Privacy Laws for establishing or maintaining an employment relationship with current or prospective FRG employees, FRG does not collect your race, ethnicity, or health Personal Information nor do we use Canadian Social Insurance Numbers (or a foreign equivalent) to identify or organize the information we hold, and will not record it if you submit it.

- **Principle Five: Limiting Use, Disclosure and Retention**
  We may only use or disclose Personal Information for the purpose for which it was collected unless you have otherwise consented, or when it is required or permitted by law. We may only retain your Personal Information for the period of time required to fulfill the purpose for which it was collected (taking into account our statutory and contractual obligations to retain information).

- **Principle Six: Accuracy**
  We shall maintain your Personal Information in as complete, accurate and up-to-date form as is necessary to fulfill the purpose for which we are to use it. Please inform us if any of your information changes by contacting us at privacy@tenthrevolution.com (for Revols: privacy@revolentgroup.com) so that we can make any necessary changes.

- **Principle Seven: Safeguarding Information**
  We must protect your Personal Information by following security safeguards that are appropriate to the sensitivity level of the Personal Information. For example, we have a document minimization process in our office to prevent inadvertent disclosures of your Personal Information. We also physically lock our offices after business hours to avoid/prevent unauthorized access. For prospective employees, FRG has an obligation to protect your privacy before, during and after the interview process, using physical, technological and organizational safeguards. Your information shall only be disclosed to persons with a 'need to know' such information for the purpose of evaluating the your suitability for employment.

- **Principle Eight: Openness**
  We are required to make information available to you that is specific and easy-to-understand concerning FRG's policies and practices that apply to the management of your Personal Information. A key method of making such information available is via this Canada Addendum.

- **Principle Nine: Access**
  Upon request to privacy@tenthrevolution.com (for Revols: privacy@revolentgroup.com), we shall inform you of the use, disclosure, and existence of your Personal Information, and shall give you access to it. You may verify the completeness and accuracy of your Personal Information, and may request amendments to your Personal Information for these reasons, if appropriate. Contact us at the email address above. We will attempt to respond to requests for summary information within 30 days of receipt. If you send us a more detailed request (typically these require archival or other retrieval costs), we may take longer to respond and you may be subject to our normal disbursement and professional fees to the highest extent permitted by applicable law.

- **Principle Ten: Challenging Compliance**
  Direct any complaints, suggestions, enquiries or questions respecting our privacy practices, compliance, or these principles by contacting privacy@tenthrevolution.com (for Revols: privacy@revolentgroup.com).

III. May We Deny Access To Your Personal Information?

Your right to access your Personal Information is not absolute. We may deny access to your Personal Information when:

- required by applicable law;
- such Personal Information relates to existing or anticipated legal proceedings against you or was generated as a result of a dispute resolution mechanism (whether arbitration, mediation, court cases, or similar proceedings);
- when granting you access would have an unreasonable impact on other people's privacy, security or proprietary information;
- to protect our rights and property; or
- where the request is frivolous or vexatious or generates costs which are prohibitively expensive.

We shall explain to you in writing why we deny a request for access to, or refuse a request to correct your Personal Information.

IV. How To Ask A Question Or File A Complaint.

FRG has a Chief Privacy Officer who may be contacted to answer any comments or questions about this Canada Addendum, including where to file a complaint. Please forward your communications to:

E-mail: privacy@tenthrevolution.com (for Revols: privacy@revolentgroup.com)
Telephone: +44 20 733 0865
Address:

Frank Recruitment Group Inc. / *Group de Recrutement Frank Inc.*
The St. Nicholas Building
St. Nicholas Street
Newcastle-Upon-Tyne
Tyne & Wear U.K. NE1 1RF
Attn: Chief Privacy Officer
Attention: Chief Privacy Officer

V. Sending Us Information Over The Internet.

With respect to CASL, by using our Websites or Services, you hereby expressly consent to receiving, during and after our business relationship, electronic messages from FRG, including via emails and through social media, providing information to you including newsletters, updates, alerts, other publications, news and communications, other information of interest to you and/or information on our services. You can withdraw this consent or modify your preferences as to the types of electronic messages which you wish to receive from us, at any time, simply by notifying us at privacy@tenthrevolution.com (for Revols: privacy@revolentgroup.com) or by using the unsubscribe mechanism on any of our electronic messages.

VI. Location of Personal Information and Transfers of Personal Information Outside Canada.

Your Personal Information is stored on various servers, including our own, and those maintained by our third party service providers who help us provide our services to you. These servers may be located outside of Canada. Accordingly, by providing us Your Personal information, you explicitly consent to our transfer of your Personal Information to countries outside of Canada. If you do not wish for your Personal Information to be transferred outside of Canada, do not provide your Personal Information to us. If you are a Quebec prospective, current, or former employee, of FRG, your employment related Personal Information is maintained by FRG Privacy, Legal, HR, and in some cases, the current/successor(s) to your line manager if lawful and appropriate under the circumstances. You have rights to access and rectification of your Personal Information, among other rights, which you may invoke as otherwise described in this Canada Addendum or this North America Privacy Policy. When we transfer your Personal Information outside of Canada, we take commercially reasonable and legally required measures with data importers as is reasonably necessary for the protection of such Personal Information, which may include entering into contractual clauses or data protection/security agreements as appropriate. As required by the Quebec Private Sector Act, in general, our server is located in the United Kingdom; our customer relationship database provider keeps its main server in Germany and its disaster recovery server in United Kingdom; our word processing and office program, email, and cloud storage provider has its main servers in the United Kingdom and the European Union; and another cloud storage provider has its main server in Ireland. For more details about your specific Personal Information and where it is located, please contact privacy@tenthrevolution.com (for Revols: privacy@revolentgroup.com).

VII. What If I Do Not Agree With This Canada Addendum?

Please do not submit any Personal Information to us if you do not agree to our processing of your Personal Information as described herein in this Canada Addendum.

VIII. Changes to this Canada Addendum

We reserve the right to change this Canada Addendum and North America Privacy Policy from time to time by updating this Canada Addendum on our website or updating the North America Privacy Policy as described above. Any changes to this Canada Addendum and North America Privacy Policy will be posted on this Website so you are always aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. We encourage you to check this Website frequently for updates. Your continued use of this Website or any FRG services shall constitute your acceptance of the revised Canada Addendum.

FRG will interpret and enforce this Canada Addendum in accordance with all applicable law.

This North America Privacy Policy was last updated on May 3, 2024.