Privacy Policy – Employees

(Effective Date: 25th May, 2018; Last Modified 4th March, 2024)

I. Introduction

Your privacy is important. This Privacy Policy (the "**Privacy Policy**") together with its addendums, the terms and conditions of your Contract of Employment, as amended from time to time (each the "**Contract of Employment**") 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 Frank Recruitment Group Services Limited and its subsidiaries, including without limitation, Nigel Frank International Limited (UK), Mason Frank International Limited (UK), Frank Recruitment Group UK Services Limited (UK), Frank Recruitment Group Services USA Ltd. (UK), Frank Recruitment Group GmbH (Germany), Frank Recruitment Group S.A. (Spain), Frank Consulting Services S.L. (Spain), Frank Recruitment Group Netherlands B.L. (Netherlands), Frank Consulting Services SAS (France), Frank Recruitment Group SRL (Italy), Frank Recruitment Group Sp z o.o. (Poland), Frank Recruitment Group Poland Sp Zo.o. (Poland), Frank Recruitment Group Sarl (Switzerland), Frank Recruitment Group Pty Limited (Australia), Frank Recruitment Group K.K. (Japan), Frank Recruitment Group Private Limited (Singapore), Frank Consulting Services Private Limited (Singapore), and (collectively, "**we**," "**us**," "**our**," or "**FRG**") collect, process, store, use, disclose and remove your personally identifiable information or personal data ("**Personal Data**" or "**PII**").

As a global document, the first part of the notice is general and applies globally (excluding North America which has its own separate North America Privacy Policy). The second part of the Privacy Policy is comprised of country-specific addendums, and where applicable, FRG will handle Personal Data relying on certain exemptions under local law, including exemptions relating to employee records. Please be sure to check the addendums to see if there is one that applies to the country in which you are working for FRG or the country(ies) of which you are a citizen or a resident. In the event of a conflict between the general part of this Privacy Policy and an addendum, the addendum prevails.

This Privacy Policy applies regardless of the form or method by which you provide Personal Data to FRG. This Privacy Policy applies to Personal Data 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 Data, how we will treat it and your rights.

The employee handbook, FRG policies or your Contract of Employment 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 Privacy Policy, on the one hand, and any FRG policy

or employee handbook or your Contract of Employment, on the other hand, the terms of this Privacy Policy shall prevail. FRG's issuance of this Privacy Policy does not otherwise change, alter, eliminate or reduce any of your or FRG's obligations under your Contract of Employment or any FRG policy or employee handbook.

II. Who are we?

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

If you want to contact FRG or any of its group companies, click **here**.

The contact details of Frank Recruitment Group's Chief Privacy Officer ("**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 Privacy Policy protect?

This Privacy Policy applies to all FRG employees who are not based in North America, regardless of which FRG affiliate is your actual employer, your title, what brand or team you work on, whether you work in "Support" or "Front Office" at FRG, what office you work in or if FRG employs you remotely. This Privacy Policy applies to Personal Data 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 Privacy Policy applies to you, you may be referred to herein as a "**Data Subject**" or collectively, "**Data Subjects**."

This 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 Data including but not limited to:

- Your name;
- Your gender;
- Your contact details e.g. email address, cell phone number, home phone number, street address;
- National insurance number, or other similar number;

- Visa number;
- Passport number;
- Superannuation details (where applicable);
- Past and present salary information;
- Bonus, stock, and other payment information;
- Company car, computer, and other company property information;
- Tax related information;
- Right-to-work status or citizenship;
- Date of birth;
- Medical or prescription drug information (if you have given your explicit consent to this data processing);
- Bank account details;
- Performance appraisals, evaluations, ratings, individual development plans, commendations, awards, disciplinary documents, individual competencies, and 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 Data, and is not covered by this Privacy Policy.

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

If FRG obtains your Personal Data from someone other than you, and if required under applicable law, FRG shall inform you of the identity and contact details of the person or entity from whom FRG obtained your Personal Data, whether FRG obtained your Personal Data from publicly available sources, the categories of Personal Data that FRG obtained and, if FRG is processing your Personal Data based on its legitimate interest (see EEA and Switzerland Addendum and UK Addendum below), the nature of FRG's legitimate interest, and shall do so by the earlier of (1) one month after FRG obtains your Personal Data or (2) if FRG uses your Personal Data to communicate with you, the first time that FRG communicates with you.

FRG shall not provide you with the information described in the paragraph immediately above if you already possess this information, providing you with such information is against (or not mandatory under) applicable law, is subject to an obligation of professional secrecy, proves impossible, would involve a disproportionate effort, or would render impossible or seriously impair the achievement of the objectives of the processing, in which case, FRG shall take appropriate measures to protect your rights, freedoms and legitimate interests.

Monitoring and Other Activities of FRG Email

Mobile Device Management. 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 Data, the Personal Data 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 intranet site and/or its human resources information system to which you have access.

No Personal Use of FRG Computer and Computer Systems – You are not permitted to use FRG's 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, networks, internet or applications from time to time.

FRG is entitled to restrict the use of company 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 company 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; and
- Protecting employees' and clients' Personal Data.

The data processing for these purposes is based a legitimate interest in processing your Personal Data, which we have balanced against your rights and freedoms and concluded that our processing is justifiable and necessary basis. Our legitimate interest is identical with the followed purpose.

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. In the event of signs of malfunctions, threats, viruses, dangerous content or violations of this Privacy Policy, your Contract of Employment , the employee handbook or any FRG policy, FRG is entitled to review, immediately and comprehensively, your use of its computers, computer systems, networks and applications as well as any logged information, especially with regard to any personal data logged and stored in this context. In the case that review results in a finding of no threats or violations of your Contract of Employment, the 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.

All emails and files sent and received through the company'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. If FRG stores any copies of the content for a period of time, FRG may delete such copies from time to time without notice.

Video/CCTV Surveillance - FRG may also engage in limited video/CCTV surveillance. 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.

With respect to your Personal Data, FRG will only take the above actions if it has a legitimate reason justifying the action and will only take the above actions with respect to the content if it has a weightier or higher justification for doing so. FRG will only take the action actions if there is no reasonable less intrusive method or measure of doing so. FRG will use reasonable efforts to avoid searching, reading or disclosing any secret or correspondence marked "private" or your other moral rights as an FRG employee.

It is possible that your Personal Data may be inadvertently monitored, intercepted, reviewed or erased by FRG while exercising its rights under this section.

It is possible that another person's personal data may be inadvertently monitored, intercepted, reviewed or erased by FRG while exercising its rights under this notice. If that is the case, FRG will make no use of such other person's personal data unless such other person consents to FRG's use of the personal data, FRG has a legitimate interest in processing such other person's data 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, phones, phone systems, databases, email

systems, applications (such as Microsoft Teams, WhatsApp, and instant messenger) and Devices for any action or use allowed by applicable law including, without limitation:

a) Processing the data or information if FRG has a legitimate interest in doing so;

b) 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.

c) 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;

d) to discipline you or any other FRG employee, up to and including dismissal;

e) to assist in determining if any supplier, contractor, candidate or client has violated FRG's contractual or other rights;

f) to protect FRG's intellectual privacy rights, company data or trade secrets;

g) to enhance FRG's compliance with applicable law or stop any potential violation of law by FRG or any other person or entity;

h) to prevent misuse of FRG computers, computer systems, phone, phone system, networks, databases, email accounts and the Device that could harm FRG;

i) to ensure compliance with our rules, standards of conduct and policies in force from time to time (including this Policy);

j) to monitor your or other FRG employees' performance at work and your compliance with your Contract of Employment;

k) 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;

l) to inspect any company confidential information, client or candidate Personal Data that is stored on any FRG printer, phone, phone system network, database, email system or application (such as Microsoft Teams, WhatsApp and instant messenger) or Device;

m) to investigate or resolve any security incident or unauthorised use of the internet at work, any FRG printer, phone, phone system, network, database, email system, application (such as Microsoft Teams, WhatsApp and instant messenger) or Device;

n) to ensure that employees do not use any FRG printer, phone, phone system, database, network, phone, phone system, email system, application (such as Microsoft Teams, WhatsApp and instant messenger) or Device for any unlawful purposes or activities that may damage our business or reputation; and

o) 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. 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 company data in all circumstances. You should therefore regularly backup any personal data contained on the device.

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

If FRG obtains your Personal Data from someone other than you, and if required under applicable law, FRG shall inform you of the identity and contact details of the person or entity from whom FRG obtained your Personal Data, whether FRG obtained your Personal Data from publicly available sources, the categories of Personal Data that FRG obtained and, if FRG is processing your Personal Data based on its legitimate interest (see EEA and Switzerland Addendum and UK Addendum below), the nature of FRG's legitimate interest, and shall do so by the earlier of (1) one month after FRG obtains your Personal Data or (2) if FRG uses your Personal Data to communicate with you, the first time that FRG communicates with you.

FRG shall not provide you with the information described in the paragraph immediately above if you already possess this information, providing you with such information is against (or not mandatory under) applicable law, is subject to an obligation of professional secrecy, proves impossible, would involve a disproportionate effort or would render impossible or seriously impair the achievement of the objectives of the processing, in which case, FRG shall take appropriate measures to protect your rights, freedoms and legitimate interests.

V. Why do we process your Personal Data?

- FRG will store, process and use your Personal Data 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 insurance, medical or other payments to you or on your behalf;
- To provide you with retirement benefits, where applicable (like personal pension plan in the UK);
- 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 internet at work and any FRG computers, computer systems, printers, phone, phone system, networks, databases, email systems, applications (such as Microsoft Teams, WhatsApp and instant messenger) and Devices;
- To extent permitted by applicable law, to monitor your compliance with your obligations under your Contract of Employment, 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 CV 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 anonymised 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 Contract of Employment;
- To enforce any of your contractual obligations to us, including those under your Contract of Employment, 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 Data 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 Contract of Employment and to draft, revise, negotiate or answer any questions you may have about your Contract of Employment, 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;
- 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 programmes 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 Data with?

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

- 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 insurance or benefits brokers, vendors, "umbrella" companies, carriers or providers;
- With third parties in connection with assisting FRG in its diversity and inclusion programmes 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 affiliates will process your Personal Data in accordance with this 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 Privacy Policy (or a similar document).

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

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

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

A breach can take many forms, including, without limitation, the loss of your Personal Data or the unauthorized access to, disclosure, modification, copying and transfer of your Personal Data.

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 Data 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 Data.

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

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

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

If so, FRG will take reasonable steps to ensure that your Personal Data is protected and treated in accordance with this Privacy Policy and local applicable law. The countries where FRG may transfer your Personal Data 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 Data are contractually bound to (a) keep your Personal Data confidential and (b) take, at a minimum, all reasonable efforts to maintain the privacy and security of your Personal Data.

Under certain circumstances, FRG may share your Personal Data with one or more of its group companies who may be located in a country other than yours or other than the country in which FRG collected your Personal Data. In such cases, FRG will comply with applicable laws and its
Intercompany Data Processing Agreements ("**DPAs**"). The DPAs are incorporated by reference into this Privacy Policy.

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

We are required by law to store your Personal Data 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 Data 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 Data over the internet

Your Personal Data 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 Privacy Policy to protect your Personal Data, 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 Privacy Policy

We reserve the right to change this Privacy Policy from time to time by updating our intranet site or internal human resources portal or website. Any changes to this 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 Privacy Policy.

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

This Privacy Policy, formerly known as a “Privacy Notice,” was first issued on 25 May, 2018.

FRG updated and amended this Privacy Policy, formerly known as a “Privacy Notice,” on 8 October, 2018, 8 September 2020, 22 September 2020, 26 February, 2021, 19 October 2021, and 8 August, 2022.

FRG updated and amended this Privacy Policy again on 4 March 2024.

Employee Certification

By signing below, I certify that I have read and understand Frank Recruitment Group’s Privacy Policy - Employees.

Printed Name

Signature

Date

UNITED KINGDOM ADDENDUM

I. Who is the Data Controller?

The Frank Recruitment Group entity who actually employs you (referred to in the following as "**we**", "**us**", "**our**" or "**FRG**") is the data controller, as defined in the United Kingdom General Data Protection Regulation ("**UK GDPR**"), with respect to your Personal Data.

II. For which purposes and how do we lawfully process your data?

In order to process your Personal Data lawfully FRG must have a legal basis to do so. FRG relies on three main legal basis for processing your Personal Data:

1) where the processing of your Personal Data is necessary for us to perform the obligations under or to enforce your obligations under, any contract between you and us, including your Contract of Employment (see A.);

2) where the processing of your Personal Data is necessary for compliance with a legal obligation to which we are subject (see B.);

3) where we have a legitimate interest in processing your Personal Data, which we have balanced against your rights and freedoms and concluded that our processing is justifiable and necessary (see C.); or

4) where we obtain your affirmative consent to use your Personal Data in this way (see D.).

We may rely on one or more legal bases to process your Personal Data.

A. Necessary for the performance of a contract

FRG has a legal basis to process your Personal Data in the performance of its contract with you, namely your Contract of Employment and to perform our obligations under our employee handbook and our policies. This basis also includes FRG's processing of your Personal Data to defend itself, bring or respond to any claims arising out of your employment and to monitor your compliance with your obligations under your Contract of Employment, our Employee handbook and our policies.

FRG relies on this legal basis to process your Personal Data for the purposes listed in Section V of the general portion of this Privacy Policy.

B. Legal obligation

In some cases, FRG has to process your Personal Data in order to comply with a legal obligation it is subject to.

In particular, the data processing for the following purposes is based on this legal basis:

- To comply with tax and social security requirements;
- To complete and submit documents required by government agencies or applicable law; and
- To cooperate with any government agency in any audit, inquiry or investigation.

C. Legitimate interest

In some cases, FRG has a legitimate interest in processing your Personal Data.

The data processing for the following purposes is based on this legal basis (our legitimate interest is identical with the followed purpose):

- To extent permitted by applicable law, to monitor or ensure your appropriate use of the internet at work and any FRG computers, computer systems, printers, phone, phone system, networks, databases, email systems, applications (such as Microsoft Teams, WhatsApp, and Messenger) and Devices;
- To extent permitted by applicable law, to monitor your compliance with your obligations under your Contract of Employment, any FRG policy or our employee handbook; and
- To cooperate with any government agency in any audit, inquiry or investigation.

D. Consent

Throughout the employment application process and during and after your employment, if any, with FRG, you may also provide FRG with express consent to process your Personal Data in order for FRG to perform specific activities for which you give consent. You can revoke your consent at any time.

III. Your Special Rights under Data Protection Laws

Your rights as a Data Subject are described in the following. FRG will provide information on action taken on a request with regard to the described rights without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. FRG will inform you of any such extension within one month of receipt of the request, together with the reasons for the delay.

If FRG does not take action on your request, FRG will inform you without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Any communication and any actions taken with regard to rights described in this section will be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, FRG may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request.

A. Do I have a right to be erased (forgotten)?

Yes. You have the right to request that FRG deletes or removes your Personal Data where there is no compelling reason for us to continue to process it. You can exercise this right by sending an email to FRG at privacy@tenthrevolution.com.

Please note that your right to erasure is not absolute. FRG will remove your Personal Data when:

(1) the Personal Data is no longer necessary in relation to the purpose for which FRG originally collected and/or processed it;

(2) FRG is processing your Personal Data on the basis of your consent and you withdraw consent;

(3) you object to the processing of your Personal Data and there is no overriding legitimate interest for us to continue to process it;

(4) the Personal Data was unlawfully processed; and

(5) the Personal Data must be erased to comply with a legal obligation.

FRG can refuse to comply with an erasure request in the following limited circumstances:

(a) to exercise FRG's right of freedom of expression and information;

(b) to comply with a legal obligation or for the performance of a public interest task;

(c) for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or

(d) for the establishment, exercise or defence of legal claims.

If we remove your Personal Data per your request for erasure, then we will confirm this with you.

If we have disclosed any of your Personal Data to a third party and you submit an erasure request to us, then we will inform (1) you about the recipients and (2) any such third parties of your erasure request unless doing so is impossible or involves disproportionate efforts.

We will respond to your erasure request without undue delay. Please note that, for your and FRG's protection, we cannot respond to an erasure request until we have verified the identity of the person making the request. This verification process may extend the response timeframes set forth in this paragraph.

B. Do I have a right of access to a copy of my Personal Data?

Yes. You have the right to:

- obtain confirmation that your Personal Data is being processed;
- a copy of your Personal Data being processed;
- the purposes of the processing;
- the categories of Personal Data being processed;
- the recipients or categories of recipients to whom FRG has disclosed your Personal Data; and
- the criteria FRG uses to determine how long it will store your Personal Data.

You can exercise this right by sending an email to FRG at privacy@tenthrevolution.com.

This right is in place to ensure that you are aware of and can verify the lawfulness of the processing.

If FRG did not collect your Personal Data from you, FRG will inform you about the source from which it obtained your Personal Data. Your right of access does not adversely affect your right of erasure (forgotten) and right of rectification, both of which are described in this addendum.

C. Do I have a right to object to the processing of my Personal Data, including the processing of my Personal Data by FRG for direct marketing?

Yes, under the following circumstances:

- You have the right to object, on grounds relating to your particular situation, to processing of your Personal Data, in case such processing is either based on our or a third party's legitimate interests or on a performance of a task carried out in the public interest. In this case, please provide us with information about your particular situation. After the assessment of the facts presented by you we will either stop processing your Personal Data or present you our compelling legitimate grounds for an ongoing processing.
- Where your Personal Data are processed for direct marketing purposes, you have the right to object at any time to the processing of your Personal Data for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where you object to processing for direct marketing purposes, the Personal Data will no longer be processed for such purposes.

You can exercise this right by sending an email to FRG at privacy@tenthrevolution.com.

If you receive a direct marketing communication from FRG and you do not wish to receive future direct marketing communications from FRG, you may request to unsubscribe from future marketing communications by sending FRG an email at privacy@tenthrevolution.com. In addition, if the direct marketing communication you received was via email, you can click the "Unsubscribe" link at the bottom of the email, fill out the required form and FRG will process your unsubscribe request. **D. Do I have a right to restrict processing of my Personal Data?**

Yes, you have a right to restrict the processing of your Personal Data. You can exercise this right by sending an email to FRG at privacy@tenthrevolution.com. When you exercise this right, FRG may continue to store your Personal Data but cannot further process it. FRG will cease processing your Personal Data in the following circumstances:

(1) when you file a rectification request with FRG (see the "Do I have a right to have any inaccurate or incomplete Personal Data rectified?" section below) in accordance with this Privacy Policy and applicable law. The restriction shall remain in place until such time as FRG has verified the accuracy of the Personal Data that is the subject of your rectification request;

(2) where FRG is processing your Personal Data based on its legitimate interest and you file a notice with FRG objecting to the processing of your Personal Data (see the "Do I have a right to object to

the processing of my Personal Data?" section above) in accordance with this Privacy Policy and applicable law, FRG will cease processing your Personal Data until such time as FRG has made a determination as to whether its legitimate grounds for continued processing override your reasons for objecting to the processing;

(3) when the processing is unlawful and you do not seek or want erasure and you file a restriction request with FRG in accordance with this Privacy Policy and applicable law instead; and

(4) if FRG no longer needs the Personal Data and you require the data to establish, exercise or defend a legal claim.

While the processing of your Personal Data is restricted, FRG may continue to process such data by storing it, processing it with your consent or processing it for the establishment, exercise or defence of legal claims.

FRG will inform you if it decides to lift a restriction on processing.

If FRG has disclosed any of your Personal Data to a third party and you submit a request to restrict processing, FRG will inform (1) you about the recipients if you so request and (2) any such third parties of your restriction request unless doing so is impossible or involves disproportionate efforts.

FRG will act on your restriction request in accordance with this Privacy Policy without undue delay. Please note that, for your and FRG's protection, FRG cannot act on a restriction request until it verifies the identity of the person making the request. This verification process may extend the timeframe in which FRG acts on your restriction request.

E. Do I have a right to Personal Data portability?

Yes**.** You can exercise this right by sending an email to FRG at privacy@tenthrevolution.com. This right exists to allow you to obtain and use your Personal Data for your own purposes across different services. Under this right, you can move, copy or transfer your Personal Data from FRG to another data controller. You will have this right where:

- the processing of your Personal Data is based on your consent or on the performance of a contract; and

- the processing is carried out by automated means.

If your portability request concerns someone other than you, FRG will have to consider whether providing or porting the Personal Data would prejudice the other person's or people's rights.

Where technically feasible, you may request that FRG transmit your Personal Data to another data controller.

F. Do I have a right to have any inaccurate or incomplete Personal Data rectified?

Yes**.** You can exercise this right by sending an email to FRG at privacy@tenthrevolution.com.

We will use reasonable endeavours to ensure that your Personal Data is maintained and up to date.

IV. What are my rights if the Security of my Personal Data is breached?

A breach of Personal Data (a "**Breach**") means a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, your Personal Data for which we are responsible under applicable law.

FRG will notify the competent supervisory authority without undue delay, and if feasible, within seventy-two (72) hours of FRG's becoming aware of the Breach, unless the Breach is unlikely to result in a risk to the rights and freedoms of natural persons.

If the Breach is likely to result in a "high risk" to your rights and freedoms, FRG will notify you without undue delay. To be clear, the threshold requiring FRG to notify you of a Breach is higher than the threshold requiring FRG to notify the competent supervisory authority of a Breach so it is possible that FRG will notify the competent supervisory authority of a Breach but not you. FRG will assess the determination of "high risk" on a case by case basis.

Any Breach notice issued by FRG will contain, where possible, (1) the categories and approximate number of individuals and Personal Data records effected by the Breach, (2) the name and contact details of the CPO (or other FRG contact representative if FRG does not have a CPO at the time that FRG issues the Breach notice), (3) a description of the likely consequences of the Breach, (4) a description of the measures that FRG has taken, and may take, to stop the Breach and, where appropriate, to mitigate the adverse effects of the Breach and (5) recommendations on actions you can take to protect yourself in light of the Breach.

V. Who do we share your personal data with?

Your personal data will be disclosed to the following third parties for the purposes mentioned above (see Section VI of the general part of this Privacy Policy.):

- insurance or benefits brokers, vendors, carriers or providers (legal basis: performance of a contract);
- retirement benefit and pension brokers, vendors, trustees or providers (legal basis: performance of a contract);

- third parties who you request data sharing with ((legal basis: your consent);
- other FRG employees whom you share your Personal Data with in the course of the performance of your job (legal basis: performance of a contract);
- government agencies in connection with any visa, tax, social security or similar issue or proceeding (legal basis: compliance with legal obligation); and
- one or more of FRG's group companies in connection with any visa, tax, social security or similar issue (legal basis: performance of a contract).

Additional information when data processors are involved. In addition, we may disclose your personal data to the following (external) contractors who assist us with specific services:

- IT-providers;
- payroll vendors and providers;
- insurance or benefits brokers, vendors, carriers or providers (legal basis: performance of a contract);
- retirement benefit and pension brokers, vendors, trustees or providers (legal basis: performance of a contract);

Such a transfer will be based on data processing agreements. Therefore, our contractors will only use your Personal Data to the extent necessary to perform their functions and will be contractually bound to process your Personal Data only on our behalf and in compliance with our requests.

In the event that we undergo re-organisation or are sold to a third party, any Personal Data we hold about you may be transferred to that re-organised entity or third party in compliance with applicable law.

We may disclose your Personal Data if legally entitled or required to do so (for example if required by law or by a court order).

Some of the recipients mentioned above reside outside the UK. For further information about cross border transfer in general and transfers outside of the UK see Section VI below.

VI. Will my Personal Data be transferred outside the UK?

FRG may transfer your Personal Data to third parties who are located outside of the UK. If so, FRG will take reasonable steps to ensure that your Personal Data is protected and treated in accordance with this Privacy Policy and local applicable law. Some of the countries outside the UK where your Personal Data may be transferred will be on the Information Commissioner's Office ("**ICO**")'s list of countries that it has deemed to have adequate security controls in place. If FRG transfers your Personal Data to a country not on this list, we will require the recipient to agree to the model clauses recognised by the ICO for data protection or other adequate safeguards (the "**Model Clauses**").

If FRG transferred any of your Personal Data to the United States ("**U.S.**") prior to 31 December 2020, you have the protections of the EU-U.S. Privacy Shield Framework and the Model Clauses. For Personal Data transferred after December 31st 2020 - October 12, 2023, you have the protections of the Model Clauses only. From October 12, 2023, you have the protections of the Model Clauses and the UK Extension to the EU-U.S. Data

Privacy Framework. FRG's U.S. subsidiaries, Frank Recruitment Group Inc. and Frank Recruitment Group Services Inc. are both registered participants in the UK Extension to the EU- U.S. Data Privacy Framework, the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (collectively, the "**DPF**"). Thus, FRG will comply with its obligations under the EU-U.S. Privacy Shield Framework and the DPF while processing any of your pre-31 December 2020 Personal Data in the U.S.

Furthermore, if you are an UK citizen or resident who FRG employs in the U.S. or who applied for employment with FRG in the U.S., prior to 31 December 2020, FRG will provide you with a copy of its U.S. Privacy Shield 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 pre-31 December 2020 Personal Data in the U.S. If you are a UK citizen or resident who FRG employs in the U.S. or who applied for employment with FRG in the U.S on or after October 12, 2023, 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 post-October 12, 2023 Personal Data in the U.S.

VII. How long will FRG store my Personal Data for?

We are required by law to store your Personal Data for 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.

With respect to the data privacy legislation applicable to the UK (i.e. the UK GDPR) (and similar laws), we will store and process your Personal Data that we obtain via (i) your consent until the earlier of (a) the purpose for which we obtained such information has been fully accomplished or (b) you inform us that you have withdrawn your consent, (ii) our legitimate interest until the earlier of (a) the purpose for which we obtained such information has been fully accomplished or (b) FRG concludes that your rights and freedoms outweigh our right to process your Personal Data and (iii) our necessity for the performance of a contract, such as the Contract of Employment, until the termination or expiration of the contract including the termination or expiration of FRG's and your respective duties or obligations under any such contract that survive any such termination or expiration.

Furthermore, we will store your Personal Data post-employment or post your application for employment for the length of time required by applicable law so that FRG can issue or respond to any claims arising out of your employment or prospective employment , or in connection with any affirmative action requirements or investigation by or of a government authority related to your employment or prospective employment.

You can email the Data Protection Officer at privacy@tenthrevolution.com

EUROPEAN ECONOMIC AREA & SWITZERLAND ADDENDUM

I. Who is the Data Controller?

The Frank Recruitment Group entity who actually employs you (referred to in the following as "**we**", "**us**", "**our**" or "**FRG**") is the data controller, as defined in the General Data Protection Regulation, including applicable Swiss law (collectively, the "**GDPR**"), with respect to your Personal Data.

II. For which purposes and how do we lawfully process your data?

In order to process your Personal Data lawfully FRG must have a legal basis to do so. FRG relies on three main legal basis for processing your Personal Data:

1) where the processing of your Personal Data is necessary for us to perform the obligations under or to enforce your obligations under, any contract between you and us, including your Contract of Employment (see A.);

2) where the processing of your Personal Data is necessary for compliance with a legal obligation to which we are subject (see B.);

3) where we have a legitimate interest in processing your Personal Data, which we have balanced against your rights and freedoms and concluded that our processing is justifiable and necessary (see C.); or

4) where we obtain your affirmative consent to use your Personal Data in this way (see D.).

We may rely on one or more legal bases to process your Personal Data.

A. Necessary for the performance of a contract

FRG has a legal basis to process your Personal Data in the performance of its contract with you, namely your Contract of Employment and to perform our obligations under our employee handbook and our policies. This basis also includes FRG's processing of your Personal Data to defend itself, bring or respond to any claims arising out of your employment and to monitor your compliance with your obligations under your Contract of Employment, our Employee handbook and our policies.

FRG relies on this legal basis to process your Personal Data for the purposes listed in Section V of the general portion of this Privacy Policy.

B. Legal obligation

In some cases, FRG has to process your Personal Data in order to comply with a legal obligation it is subject to.

In particular, the data processing for the following purposes is based on this legal basis:

- To comply with tax and social security requirements;
- To complete and submit documents required by government agencies or applicable law; and
- To cooperate with any government agency in any audit, inquiry or investigation.

C. Legitimate interest

In some cases, FRG has a legitimate interest in processing your Personal Data.

The data processing for the following purposes is based on this legal basis (our legitimate interest is identical with the followed purpose):

- To extent permitted by applicable law, to monitor or ensure your appropriate use of the internet at work and any FRG computers, computer systems, printers, phone, phone system, networks, databases, email systems, applications (such as Microsoft Teams, WhatsApp, and Messenger) and Devices;
- To extent permitted by applicable law, to monitor your compliance with your obligations under your Contract of Employment, any FRG policy or our employee handbook; and
- To cooperate with any government agency in any audit, inquiry or investigation.

D. Consent

Throughout the employment application process and during and after your employment, if any, with FRG, you may also provide FRG with express consent to process your Personal Data in order for FRG to perform specific activities for which you give consent. You can revoke your consent at any time.

III. Your Special Rights under Data Protection Laws

Your rights as a Data Subject are described in the following. FRG will provide information on action taken on a request with regard to the described rights without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. FRG will inform you of any such extension within one month of receipt of the request, together with the reasons for the delay.

If FRG does not take action on your request, FRG will inform you without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Any communication and any actions taken with regard to rights described in this section will be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, FRG may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request.

A. Do I have a right to be erased (forgotten)?

Yes. You have the right to request that FRG deletes or removes your Personal Data where there is no compelling reason for us to continue to process it. You can exercise this right by sending an email to FRG at privacy@tenthrevolution.com.

Please note that your right to erasure is not absolute. FRG will remove your Personal Data when:

(1) the Personal Data is no longer necessary in relation to the purpose for which FRG originally collected and/or processed it;

(2) FRG is processing your Personal Data on the basis of your consent and you withdraw consent;

(3) you object to the processing of your Personal Data and there is no overriding legitimate interest for us to continue to process it;

(4) the Personal Data was unlawfully processed; and

(5) the Personal Data must be erased to comply with a legal obligation.

FRG can refuse to comply with an erasure request in the following limited circumstances:

(a) to exercise FRG's right of freedom of expression and information;

(b) to comply with a legal obligation or for the performance of a public interest task;

(c) for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or

(d) for the establishment, exercise or defence of legal claims.

If we remove your Personal Data per your request for erasure, then we will confirm this with you.

If we have disclosed any of your Personal Data to a third party and you submit an erasure request to us, then we will inform (1) you about the recipients and (2) any such third parties of your erasure request unless doing so is impossible or involves disproportionate efforts.

We will respond to your erasure request without undue delay. Please note that, for your and FRG's protection, we cannot respond to an erasure request until we have verified the identity of the person making the request. This verification process may extend the response timeframes set forth in this paragraph.

B. Do I have a right of access to a copy of my Personal Data?

Yes. You have the right to:

- obtain confirmation that your Personal Data is being processed;
- a copy of your Personal Data being processed;
- the purposes of the processing;
- the categories of Personal Data being processed;
- the recipients or categories of recipients to whom FRG has disclosed your Personal Data; and
- the criteria FRG uses to determine how long it will store your Personal Data.

You can exercise this right by sending an email to FRG at privacy@tenthrevolution.com.

This right is in place to ensure that you are aware of and can verify the lawfulness of the processing.

If FRG did not collect your Personal Data from you, FRG will inform you about the source from which it obtained your Personal Data. Your right of access does not adversely affect your right of erasure (forgotten) and right of rectification, both of which are described in this addendum.

C. Do I have a right to object to the processing of my Personal Data, including the processing of my Personal Data by FRG for direct marketing?

Yes, under the following circumstances:

- You have the right to object, on grounds relating to your particular situation, to processing of your Personal Data, in case such processing is either based on our or a third party's legitimate interests or on a performance of a task carried out in the public interest. In this case, please provide us with information about your particular situation. After the assessment of the facts presented by you we will either stop processing your Personal Data or present you our compelling legitimate grounds for an ongoing processing.
- Where your Personal Data are processed for direct marketing purposes, you have the right to object at any time to the processing of your Personal Data for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where you object to processing for direct marketing purposes, the Personal Data will no longer be processed for such purposes.

You can exercise this right by sending an email to FRG at privacy@tenthrevolution.com.

If you receive a direct marketing communication from FRG and you do not wish to receive future direct marketing communications from FRG, you may request to unsubscribe from future marketing communications by sending FRG an email at privacy@tenthrevolution.com. In addition, if the direct marketing communication you received was via email, you can click the "Unsubscribe" link at the bottom of the email, fill out the required form and FRG will process your unsubscribe request.

D. Do I have a right to restrict processing of my Personal Data?

Yes, you have a right to restrict the processing of your Personal Data. You can exercise this right by sending an email to FRG at privacy@tenthrevolution.com. When you exercise this right, FRG may continue to store your Personal Data but cannot further process it. FRG will cease processing your Personal Data in the following circumstances:

(1) when you file a rectification request with FRG (see the "Do I have a right to have any inaccurate or incomplete Personal Data rectified?" section below) in accordance with this Privacy Policy and applicable law. The restriction shall remain in place until such time as FRG has verified the accuracy of the Personal Data that is the subject of your rectification request;

(2) where FRG is processing your Personal Data based on its legitimate interest and you file a notice with FRG objecting to the processing of your Personal Data (see the "Do I have a right to object to the processing of my Personal Data?" section above) in accordance with this Privacy Policy and applicable law, FRG will cease

processing your Personal Data until such time as FRG has made a determination as to whether its legitimate grounds for continued processing override your reasons for objecting to the processing;

(3) when the processing is unlawful and you do not seek or want erasure and you file a restriction request with FRG in accordance with this Privacy Policy and applicable law instead; and

(4) if FRG no longer needs the Personal Data and you require the data to establish, exercise or defend a legal claim.

While the processing of your Personal Data is restricted, FRG may continue to process such data by storing it, processing it with your consent or processing it for the establishment, exercise or defence of legal claims.

FRG will inform you if it decides to lift a restriction on processing.

If FRG has disclosed any of your Personal Data to a third party and you submit a request to restrict processing, FRG will inform (1) you about the recipients if you so request and (2) any such third parties of your restriction request unless doing so is impossible or involves disproportionate efforts.

FRG will act on your restriction request in accordance with this Privacy Policy without undue delay. Please note that, for your and FRG's protection, FRG cannot act on a restriction request until it verifies the identity of the person making the request. This verification process may extend the timeframe in which FRG acts on your restriction request.

E. Do I have a right to Personal Data portability?

Yes**.** You can exercise this right by sending an email to FRG at privacy@tenthrevolution.com. This right exists to allow you to obtain and use your Personal Data for your own purposes across different services. Under this right, you can move, copy or transfer your Personal Data from FRG to another data controller. You will have this right where:

- the processing of your Personal Data is based on your consent or on the performance of a contract; and
- the processing is carried out by automated means.

If your portability request concerns someone other than you, FRG will have to consider whether providing or porting the Personal Data would prejudice the other person's or people's rights.

Where technically feasible, you may request that FRG transmit your Personal Data to another data controller.

F. Do I have a right to have any inaccurate or incomplete Personal Data rectified?

Yes**.** You can exercise this right by sending an email to FRG at privacy@tenthrevolution.com.

We will use reasonable endeavours to ensure that your Personal Data is maintained and up to date.

IV. What are my rights if the Security of my Personal Data is breached?

A breach of Personal Data (a "**Breach**") means a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, your Personal Data for which we are responsible under applicable law.

FRG will notify the competent supervisory authority without undue delay, and if feasible, within seventy two (72) hours of FRG's becoming aware of the Breach, unless the Breach is unlikely to result in a risk to the rights and freedoms of natural persons.

If the Breach is likely to result in a "high risk" to your rights and freedoms, FRG will notify you without undue delay. To be clear, the threshold requiring FRG to notify you of a Breach is higher than the threshold requiring FRG to notify the competent supervisory authority of a Breach so it is possible that FRG will notify the competent supervisory authority of a Breach but not you. FRG will assess the determination of "high risk" on a case by case basis.

Any Breach notice issued by FRG will contain, where possible, (1) the categories and approximate number of individuals and Personal Data records effected by the Breach, (2) the name and contact details of the CPO (or other FRG contact representative if FRG does not have a CPO at the time that FRG issues the Breach notice), (3) a description of the likely consequences of the Breach, (4) a description of the measures that FRG has taken, and may take, to stop the Breach and, where appropriate, to mitigate the adverse effects of the Breach and (5) recommendations on actions you can take to protect yourself in light of the Breach.

V. Who do we share your personal data with?

Your personal data will be disclosed to the following third parties for the purposes mentioned above (see Section VI of the general part of this Privacy Policy.):

- insurance or benefits brokers, vendors, carriers or providers (legal basis: performance of a contract);
- retirement benefit and pension brokers, vendors, trustees or providers (legal basis: performance of a contract);
- third parties who you request data sharing with ((legal basis: your consent);
- other FRG employees whom you share your Personal Data with in the course of the performance of your job (legal basis: performance of a contract);
- government agencies in connection with any visa, tax, social security or similar issue or proceeding (legal basis: compliance with legal obligation); and
- one or more of FRG's group companies in connection with any visa, tax, social security or similar issue (legal basis: performance of a contract).

Additional information when data processors are involved. In addition, we may disclose your personal data to the following (external) contractors who assist us with specific services:

- IT-providers;
- payroll vendors and providers;
- insurance or benefits brokers, vendors, carriers or providers (legal basis: performance of a contract);
- retirement benefit and pension brokers, vendors, trustees or providers (legal basis: performance of a contract);

Such a transfer will be based on data processing agreements. Therefore, our contractors will only use your Personal Data to the extent necessary to perform their functions and will be contractually bound to process your Personal Data only on our behalf and in compliance with our requests.

In the event that we undergo re-organisation or are sold to a third party, any Personal Data we hold about you may be transferred to that re-organised entity or third party in compliance with applicable law.

We may disclose your Personal Data if legally entitled or required to do so (for example if required by law or by a court order).

Some of the recipients mentioned above reside outside the EEA/Switzerland. For further information about cross border transfer in general and transfers outside of the EEA/Switzerland see Section VI below.

VI. Will my Personal Data be transferred outside the EEA/Switzerland?

FRG may transfer your Personal Data to third parties who are located outside of the EEA/Switzerland. If so, FRG will take reasonable steps to ensure that your Personal Data is protected and treated in accordance with this Privacy Policy and local applicable law. Some of the countries outside the EEA/Switzerland where your Personal Data may be transferred will be on the EU Commission's or Swiss Federal Data Protection and Information Commissioner's ("**SFDPIC**") respective lists of countries deemed to have adequate security controls in place. If FRG transfers your Personal Data to a country not on these lists, we will require the recipient to agree to the EU Commission's or SFDPIC's model clauses, as applicable, for data protection or other adequate safeguards.

If FRG transfers any of your Personal Data to the United States, FRG's U.S. subsidiaries, Frank Recruitment Group Inc. and Frank Recruitment Group Services Inc. are both registered participants in the EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework(s) (collectively, the "**DPF**") . Thus, FRG will comply with its obligations under the DPF while processing any of your Personal Data in the U.S.

Furthermore, if you are an EEA or Swiss citizen or resident who FRG employs in the U.S. or who applied for employment with FRG in the U.S., 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 Data in the U.S.

VII. How long will FRG store my Personal Data for?

We are required by law to store your Personal Data for 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.

With respect to the data privacy legislation applicable to the countries in the EEA/Switzerland (i.e. the GDPR) (and similar laws), we will store and process your Personal Data that we obtain via (i) your consent until the earlier of (a) the purpose for which we obtained such information has been fully accomplished or (b) you inform us that you have withdrawn your consent, (ii) our legitimate interest until the earlier of (a) the purpose for which we obtained such information has been fully accomplished or (b) FRG concludes that your rights and freedoms outweigh our right to process your Personal Data and (iii) our necessity for the performance of a contract, such as the Contract of Employment, until the termination or expiration of the contract including the termination or expiration of FRG's and your respective duties or obligations under any such contract that survive any such termination or expiration.

Furthermore, we will store your Personal Data post-employment or post your application for employment for the length of time required by applicable law so that FRG can issue or respond to any claims arising out of your employment or prospective employment , or in connection with any affirmative action requirements or investigation by or of a government authority related to your employment or prospective employment.

FRG's Data Protection Officer is Steven Lawton. You can email the Data Protection Officer at privacy@tenthrevolution.com

GERMANY ADDENDUM

This Germany Addendum applies to German employees and prospective employees in addition to the European Economic Area and Switzerland Addendum above. Notwithstanding anything to the contrary therein in the European Economic Area and Switzerland Addendum above, FRG shall not monitor your use of FRG's computer systems, email or telephone without your prior written consent except to determine if you are complying FRG policies, including this Policy. FRG shall not install any mobile device management products on FRG equipment that you use or any equipment owned or leased by you.

ITALIAN ADDENDUM

For avoidance of doubt, this Italy Addendum applies to Italian employees and prospective employees in addition to the European Economic Area and Switzerland Addendum above. Notwithstanding anything to the contrary therein in the European Economic Area and Switzerland Addendum above, in monitoring your use of FRG's computer systems, email or telephone through any authorized software, FRG shall comply with Article 4 of Italian Law no. 300/1970 and subsequent amendments. You are informed that, according to Article 4 of Italian Law no. 300/1970, FRG is entitled to process and use all information obtained from devices given to you for performing the working activity. FRG is therefore entitled to use the information obtained from those devices for any purpose linked to the employment relationship.

JAPANESE ADDENDUM

Frank Recruitment Group 株式会社 (以下「当社」) は登録者の個人情報の取り扱いについては個人情報保護法及びＪＩＳQ15001：2006 に基づき 適正な管理に努めてまいります。

Frank Recruitment Group K.K (hereinafter referred to as "FRG") will endeavor to properly manage the handling of personal information of registrants based on the Act on the Protection of Personal Information and JISQ15001: 2006.

ここでいう個人情報とは、当社に提供する個人 (以下「本人」という) に関する情報で、氏名、住所、生年月日、電話番号、メールアドレス、その他の記述の組み合わせにより本人を特定できる情報をいいます。We are still working on our Policy and will publish updates soon. Please check back frequently for updates.

私たちはまだポリシーに取り組んでおり、すぐに更新を公開します.最新情報を頻繁に確認してください。

お預かりした個人情報につきまして、利用目的の通知、開示、訂正、追加、削除、利用停止をご希望の場合は、ご本人であることを確認させていただいた上で速やかに対応いたします。

If you wish to notify, disclose, correct, add, delete, or suspend the use of your personal information, we will promptly respond after confirming your identity.

お気軽にお問い合わせください

Please feel free to contact us on;

Frank Recruitment Group 株式会社への個人情報に関するお問い合わせ窓口

TEL：03-4563-8890

E メール privacy@tenthrevolution.com

※本同意書の効力、適用、解釈にあたっては、日本国法が適用されるものとします。

制定日　２０XX 年 XX 月 XX 日

SINGAPORE ADDENDUM

1. INTRODUCTION TO THE PERSONAL DATA PROTECTION ACT 2012 (“PDPA”)

1.1 “Personal Data” is defined under the PDPA to mean data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which an organisation has or is likely to have access.

1.2 We will collect your Personal Data in accordance with the PDPA. In general, before we collect any Personal Data from you, we will notify you of the purposes for which your Personal Data may be collected, used and/or disclosed, as well as obtain your consent for the collection, use and/or disclosure of your Personal Data for the intended purposes.

1.3 Your Personal Data may also be collected, used or disclosed if we have assessed that to do so would be in our legitimate interests and beneficial to the public. Before doing so, we will take steps to ensure that any adverse effects that might arise for you have already been identified and eliminated, reduced or mitigated.

2. PURPOSES FOR COLLECTION, USE & DISCLOSURE OF PERSONAL DATA

2.1 The Personal Data which we collect from you may be collected, used and/or disclosed for the following purposes:

(a) facilitating, processing, dealing with, administering, and/or managing your employment with FRG.

(b) processing and/or administering any consultations, negotiations, and an a suitable placement within FRG

(c) processing and/or administering requests for access and/or correction of your Personal Data;

(d) processing your registration and/or participation for seminars, exhibitions, and other events organized or co-organized by FRG;

(e) carrying out your instructions or responding to any enquiry given by (or purported to be given by) you or on your behalf;

(f) conducting employee due diligence or other screening and personal identification in accordance with laws, regulations or our risk management procedures that may be required by law or that may have been put in place by us;

(g) to prevent or investigate any fraud, unlawful activity or omission or misconduct, whether or not there is any suspicion of the aforementioned;

(h) complying with or as required by any applicable law, governmental or regulatory requirements of any relevant jurisdiction, including meeting the requirements to make disclosure under the requirements of any law binding on us and/or for the purposes of any guidelines issued by regulatory or other authorities, whether in Singapore or elsewhere, with which we are expected to comply;

(i) complying with or as required by any request or direction of any governmental authority, or responding to requests for information from public agencies, ministries, statutory boards or other

similar authorities. For the avoidance of doubt, this means that we may/will disclose your Personal Data to the aforementioned parties upon their request or direction; etc.

(collectively, the “Purposes”).

1.1 To conduct our business operations more smoothly, we may also be disclosing the Personal Data you have provided to us to our third-party service providers which may be sited outside of Singapore, for one or more of the above-stated purposes. This is because such third-party service providers, agents and/or affiliates or related corporations would be processing your Personal Data on our behalf for one or more of the above-stated purposes.

3. SPECIFIC ISSUES FOR THE DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

3.1 We respect the confidentiality of the Personal Data you have provided to us.

3.2 In that regard, we will not disclose any of your Personal Data to any third parties without first obtaining your express consent permitting us to do so. However, please note that we may disclose your Personal Data to third parties without first obtaining your consent in certain situations, including, without limitation, the following:

(a) cases in which the disclosure is required based on the applicable laws and/or regulations;

(b) cases in which the purpose of such disclosure is clearly in your interests (Legitimate Interest), and if consent cannot be obtained in a timely way, provided that we shall, as soon as may be practicable, notify you of the disclosure and the purposes of the disclosure;

(c) cases in which the disclosure is necessary to respond to an emergency that threatens the life, health or safety of yourself or another individual;

(d) cases in which there are reasonable grounds to believe that the health or safety of yourself or another individual will be seriously affected and consent for the disclosure of the data cannot be obtained in a timely way, provided that we shall, as soon as may be practicable, notify you of the disclosure and the purposes of the disclosure;

(e) cases in which the disclosure is necessary for any investigation or proceedings as required by law;

(f) cases in which the Personal Data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorisation signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the Personal Data is necessary for the purposes of the functions or duties of the officer; and/or

(g) cases in which the disclosure is to a public agency and such disclosure is necessary in the public interest.

3.3 The instances listed above at paragraph 3 are not intended to be exhaustive. For an exhaustive list of exceptions, you are encouraged to peruse the First and Second Schedules of the PDPA which is publicly available at https://sso.agc.gov.sg/.

3.4 In all other instances of disclosure of Personal Data to third parties with your express consent, we will endeavour to provide adequate supervision over the handling and administration of your Personal Data by such third parties, as well as to provide for adequate forms of protection over such Personal Data.

3.5 Where Personal Data is transferred by us to any third parties outside of Singapore, we will ensure that such transfers are compliant with the requirements under the PDPA. In this regard, we will take such necessary measures to ensure that such overseas recipients are bound by legally enforceable obligations to ensure that these overseas recipients provide a standard of protection to the Personal Data so transferred that is comparable to the protection under the PDPA.

4. REQUEST FOR ACCESS AND/OR CORRECTION OF PERSONAL DATA

Access Request

4.1 An individual may request for us to provide access to Personal Data about the individual that is in our possession or under our control as well as information about the ways in which the Personal Data has been used or disclosed by us within a year before the date of the request.

4.2 Unless an exception to the access request applies, we will respond to your access request as soon as reasonably possible from the time the access request is received. If we are unable to respond to an access request within thirty (30) days after receiving the request, we shall inform you in writing within the thirty (30) day period, of the reasonably soonest time in which we will respond.

Correction Request

4.3 An individual may also request for us to correct Personal Data that is in our possession or under our control. Unless an exception to the correction request applies, or we are satisfied on reasonable grounds that a correction should not be made, we will endeavour to correct the Personal Data as soon as practicable and send the corrected Personal Data to every other organisation to which the Personal Data was disclosed by us within a year before the date the correction was made. This is unless that other organisation does not need the corrected Personal Data for any legal or business purpose.

4.4 Where we are unable to respond to a correction request within thirty (30) days after receiving the request, we shall inform you in writing within the thirty (30) day period, of the reasonably soonest time in which we will respond.

4.5 You may submit your access or correction request to the contact details listed at paragraph 7.2 of this Singapore Addendum.

5. REQUEST TO WITHDRAW CONSENT

5.1 You may withdraw your consent for the collection, use and/or disclosure of your Personal Data in our possession or under our control at any time by submitting your request to the contact details listed at paragraph 7.2 of this Singapore Addendum.

5.2 We will process your request as soon as practicable such a request for withdrawal of consent being made, and will thereafter refrain from collecting, using and/or disclosing your Personal Data in the manner stated in your request.

6. ADMINISTRATION AND MANAGEMENT OF PERSONAL DATA

6.1 We will take appropriate measures to keep your Personal Data accurate, complete and updated.

6.2 We will also take commercially reasonable efforts to take appropriate precautions and preventive measures to ensure that your Personal Data is adequately protected and secured. Appropriate security arrangements will be taken to prevent any unauthorised access, collection, use, disclosure, copying, modification, leakage, loss, damage and/or alteration of your Personal Data. However, we cannot assume responsibility for any unauthorised use of your Personal Data by third parties which are wholly attributable to factors beyond our control.

6.3 We will also take commercially reasonably efforts to ensure that the Personal Data in our possession or under our control is destroyed and/or anonymised as soon as it is reasonable to assume that (i) the purpose for which that Personal Data was collected is no longer being served by the retention of such Personal Data; and (ii) retention is no longer necessary for any other legal or business purposes.

7. COMPLAINT PROCESS

7.1 If you have any complaint or grievance regarding about how we are handling your Personal Data or about how we are complying with the PDPA, we welcome you to contact us with your complaint or grievance.

7.2 Please contact us at privacy@tenthrevolution.com

7.3 Where it is an email or a letter through which you are submitting a complaint, your indication at the subject header that it is a PDPA complaint would assist us in attending to your complaint speedily by passing it on to the privacy department to handle. For example, you could insert the subject header as “PDPA Complaint”.

7.4 We will certainly strive to deal with any complaint or grievance that you may have speedily and fairly.

2 UPDATES ON PRIVACY STATEMENT

2.1 As part of our efforts to ensure that we properly manage, protect and process your Personal Data, we will be reviewing our policies, procedures and processes from time to time.

2.2 We reserve the right to amend the terms of this Singapore Addendum at our absolute discretion. Any amended Singapore Addendum will be posted on our website and can be viewed at www.tenthrevolution.com

2.3 You are encouraged to visit the above website from time to time to ensure that you are well informed of our latest privacy policy.

AUSTRALIA ADDENDUM

In this notice, Personal Data has the same meaning as "Personal Information" under the *Privacy Act 1988* (Cth). When we handle your Personal Data, we will do so in accordance with Australian privacy requirements, including any exemptions for employee records that apply under Australian privacy laws.

You are also notified that:

a) your Personal Data will be held and processed overseas including in the United States, the United Kingdom, the European Economic Area or Singapore where our offices are located and other countries in which we may open offices. We may also disclose your personal information to others, like our consultants, agents, contractors and service providers, and those that act as data processors, auditors or external advisers, and may be held and processed in countries including those listed in the beginning of this subsection "a";

b) we may collect Personal Data about you, where lawful to do so, from your use of FRG's computer systems and resources which are provided and maintained by FRG for its business purposes, and made available to you for the performance of your work. Please ensure that you read FRG's policies and/or Employee handbook carefully outlining the conditions for acceptable use of FRG's computer systems and resources. We will comply with any obligations that apply to collection of your Personal Data under workplace surveillance legislation in Australia;

c) If we use your Personal Data to contact you and you would prefer us not to, or if you indicate a preference for a method of communication, please let us know and we will do our best to respect your preference. When your choice is to continue to deal with us, we take it that you agree to and consent to us using your personal information in these ways, providing we follow the system and approach we explain in this Privacy Policy and comply with applicable law. Where we do not have your Personal Data, we are not able to contact you, process your requests or employment application, carry out FRG's human resource management functions (including the provision of employee benefits), or provide our services to you; and

d) the governing law for the purposes of the Privacy Policy, and any matters relating to them, including all disputes, will be the laws of Victoria, Australia. You unconditionally submit to the nonexclusive jurisdiction of the courts having jurisdiction there.

You may wish to contact us to request access to your Personal Data, to seek to correct it or to make a complaint about privacy. Our contact details are set out below:

Frank Recruitment Group Pty Ltd
222 Exhibition Street, Level 9
Melbourne, Victoria, Australia 3000
Email: privacy@tenthrevolution.com

Our Chief Privacy Officer will respond to your request for access to Personal Data we hold about you as soon as we reasonably can, including if we are unable to provide you with access (such as when we no longer hold the information).

We do not impose any charge for a request for access, but we may charge you a reasonable fee for our costs associated with providing you with access and retrieval costs.

For complaints about privacy, we will establish in consultation with you a reasonable process, including timeframes, for seeking to resolve your complaint.