**Privacy Policy Statement**

1. INTRODUCTION

1.1. This Statement is adopted as the Privacy Policy Statement (this "Statement") of Finrate AG, Switzerland (the "Company"). The purpose of this Statement is to establish the policies and practices of the Company's commitment to protect the privacy of personal data and to act in compliance with applicable laws and guidelines in jurisdictions where the Company operates.

1.2. The Company's subsidiaries have their own policies and practices to ensure full compliance with the applicable legal and regulatory requirements in their respective jurisdictions relating to personal data protection.

1.3. This Statement may be reviewed and amended from time to time, to take into account changes in legislation that may occur, and/or guidance from the relevant regulatory authority, and/or changes in technology which may affect how personal data is collected, used and/or disclosed.

2. CATEGORIES OF PERSONAL DATA HELD BY THE COMPANY

2.1. There are two broad categories of personal data held by the Company: (1) personal data related to customers and (2) personal data related to employees/potential employees of the Company.

2.2. Personal data held by the Company relating to customers includes personal data of customers (where they are individuals). Such personal data may include the following:

2.2.1. their name, contact details (including email address, user name and password;

2.2.2. information obtained by the Company in the ordinary course of its business relationship with customers (for example, when customers use the Company's services, the data from their usage of the Services such as timestamps, and communicate verbally or in writing with the Company, by means of emails, documentation, digital conversations (such as through WhatsApp chats or similar software) or telephone recording systems as the case may be); and

2.2.3. information which is in the public domain.

2.3. Personal data held by the Company regarding employees and potential employees may include the following:

2.3.1. name and address, contact details, date of birth and nationality of employees and potential employees and their dependents and their identity card and/or passport numbers and place and date of issue thereof;

2.3.2. CVs and application forms, recruitment assessment documents such as interview notes and additional information compiled about potential employees to assess their suitability for a job in the course of the recruitment and selection process which may include references obtained from their current or former employers or other sources;

2.3.3. offer letters and employment / engagement contracts;

2.3.4. records of pre-employment / pre-engagement security checks such as proof of the right to work, proof of residence, financial sanctions records and reference responses;

2.3.5. professional training and education details, employee attendance at training sessions as well as any feedback employees provide / provided at those sessions;

2.3.6. financial information including payroll records, salary and benefits (including for example, bank account details, expenses, salary, benefits and bonuses);

2.3.7. employee opinions / views on working at the Company whether as a new starter or during an exit interview or during periodic engagement surveys;

2.3.8. relevant personal data pertaining to former employees required by the Company to fulfil its obligations to the former employees and its legal obligations under certain ordinances, laws and regulatory guidance and guidelines;

2.3.9. emergency contact details;

2.3.10. holiday, sickness absence, paid leave, unpaid leave, maternity, paternity, adoption, shared parental leave and parental leave records;

2.3.11. performance reviews;

2.3.12. redundancy or redeployment records;

2.3.13. medical information employees provide as part of health and safety returns, accident reports and related details, medical notes and records (including disabilities, any reasonable adjustments required and occupational health assessments);

2.3.14. personal data contained in employees' work including in emails and other documents as well as personal telephone, email and address records;

2.3.15. records of employee's use of the Company's facilities, network, premises, information or documents and IT systems, IT equipment, telephone access records;

2.3.16. information the Company receives about employees as part of the Company's compliance requirements;

2.3.17. diversity monitoring information;

2.3.18. images such as photographs and CCTV recordings;

2.3.19. additional information compiled about employees in the ordinary course of the continuation of the employment relationship; and

2.3.20. information which is available in the public domain.

2.4. In addition to the above, the Company may hold other kinds of personal data which it needs in light of experience and the specific nature of its business.

## 3. PURPOSES THE PERSONAL DATA IS COLLECTED, HELD, USED AND/OR DISCLOSED

3.1. All personal data collected will only be used for purposes which are directly related to and reasonably appropriate for the Company's functions or activities. The Company will seek the consent of the individuals before collecting any personal data and before using the personal data for the purposes listed in paragraphs 3.5 and 3.6 respectively, except where permitted or authorised by law. The Company will also seek the consent of the individuals before collecting any additional personal data and before using the personal data for a purpose which has not been notified to the individuals (except where permitted or authorised by law). Personal data collected may be transferred to third parties when necessary for the same purposes. Individuals concerned would be informed of the possible transferees of their personal data when their personal data is collected.

3.2. The Company is not required to specify every activity which it may undertake so long as it has provided sufficient detail for the individual to determine the objectives or reasons for which the Company is collecting, using and/or disclosing personal data (as the case may be).

3.3. It is necessary for customers to supply the Company with data to enable the Company to provide or continue to provide the cloud services relating to stakeholder management (which may include data room access and storage, access tracking, board management and digital equity management solutions, and tracking of employees and prospective employees of the customer ("Services").

3.4. It is also the case that data is collected from customers in the ordinary course of the Company's provision of, and continuation of provision of, the Services.

3.5. The purposes for which data relating to customers may be collected, used and disclosed are as follows:

3.5.1. For the purpose of supplying the Company's Services: that customers have requested from the Company via the Company website. The Company may collect and process personal data whether customers are interacting with us on their own behalf or on behalf of any organisation that they represent. The Company may process this information so that it can fulfil the supply of Services, maintain the Company database, process user accounts and user login information to identify users and grant access to secure areas of the Company website, and to keep a record of how Services are being used;

3.5.2. To communicate with customers (as applicable), including but not limited to:

(a) operational communications, to administer user accounts and contact users regarding their account, changes to the Company website and Services, security updates, customer service and general enquiries assistance (by email, telephone, or via a "live chat" function) with using the Company website and Services;

(b) marketing communications (about the Company or another product or service which the Company considers a user might be interested in) in accordance with their marketing preferences, including notifying them of Company marketing events, initiatives, and other promotions; and

(c) asking for feedback on the Services or to take part in any research the Company is conducting (which the Company may engage a third party to assist with);

3.5.3. To support customers (as applicable): this may include assisting with the resolution of technical support issues or other issues relating to the websites or Services, whether by email, online support or otherwise;

3.5.4. To analyse, aggregate and report: the Company may use the personal data it collects about customers through the Company websites and Services (whether obtained directly or from third parties) to produce aggregated and anonymised analytics and reports, which the Company may share publicly or with third parties;

3.5.5. Behavioural Tracking: the Company may, in connection with the provision of certain services (such as hosting and providing access to online data rooms on the Company's platform), collect information about how customers interact with the online platform. Such collection may involve tracking and recording the time and date of the access, the specific functionality that may have been utilized by the specific Customer, as well as other personal data in relation to their interaction with the platform. The Company may share such data collected with specific third parties that provide services such as accounting, legal, project management, business planning, HR management, recruitment, and employee training;

3.5.6. To improve the Company website and Services and develop new ones: for example, by tracking and monitoring users use of the website and Services so we can keep improving, or by carrying out technical analysis of the Company's website and Services so that we can modify user experience and provide users with more efficient tools and new services;

3.5.7. To link and interact with other sites (such as LinkedIn, Twitter and other social media and file sharing sites) including: linking to these pages and interacting with any 'like' or similar embedded features on the Company website or social media accounts, the Company and the relevant social media platform may receive information relating to such interaction and may share personal data in connection with this purpose;

3.5.8. Marketing Services, products and other subjects (please see further details in paragraph (4) of the Company's Personal Information Collection (Customers) Statement);

3.5.9. Verification of the data or information provided by any other customer or third party;

3.5.10. Enforcing customers' obligations;

3.5.11. Compliance with laws: Complying with the obligations, requirements or arrangements for disclosing and using data that apply to the Company or any of its subsidiaries or that it is expected to comply according to:

(a) any law binding or applying to it within or outside the jurisdictions in which the Company operates existing currently and in the future; and

(b) any guidelines or guidance given or issued by any legal, regulatory, governmental, tax, law enforcement or other authorities, or self-regulatory or industry bodies or associations of financial services providers within or outside the jurisdictions in which the Company operates existing currently and in the future; and

(c) any present or future contractual or other commitment with local or foreign legal, regulatory, governmental, tax, law enforcement or other authorities, or self-regulatory or industry bodies or associations that is assumed by or imposed on the Company or any of its subsidiaries by reason of its financial, commercial, business or other interests or activities in or related to the jurisdiction of the relevant local or foreign legal, regulatory, governmental, tax, law enforcement or other authority, or self-regulatory or industry bodies or associations;

3.5.12. Compliance with internal policies: complying with any obligations, requirements, policies, procedures, measures or arrangements for sharing data and information within the group of the Company and/or any other use of data and information in accordance with any group-wide programmes for compliance with sanctions or prevention or detection of money laundering, terrorist financing or other unlawful activities.

3.5.13. Due diligence: enabling an actual lender, investor or proposed assignee of the Company, or participant or sub-participant of the Company's rights in respect of the customer to evaluate the transaction intended to be the subject of the lending, investment, assignment, participation or sub-participation.

3.5.14. General: purposes related to or furthering any of the purposes set out in the foregoing sub-paragraphs in this paragraph 3.5.

3.6. The purposes for which data relating to employees and potential employees may be collected, used and disclosed are as follows:

3.6.1. processing employment applications;

3.6.2. payroll administration and other financial, regulatory, insurance and taxation related matters including those handled or facilitated by the Company on behalf of its employees;

3.6.3. determining, reviewing or allocating salaries, bonuses and other benefits including industry benchmarking activities;

3.6.4. conducting fit and proper assessment and performance assessment according to internal policy or regulatory requirements or consideration of promotion, training, secondment or transfer;

3.6.5. determining any disciplinary or rectifying action arising from employees' conduct or employees' ability to perform their job requirements;

3.6.6. consideration of eligibility for and administration of staff loans and other benefits and entitlements;

3.6.7. diversity and equal opportunity monitoring;

3.6.8. manpower and succession planning;

3.6.9. sickness absence monitoring and reporting;

3.6.10. health and safety monitoring (including accident reporting);

3.6.11. performance reviews and management;

3.6.12. learning and training sessions and subsequent reporting;

3.6.13. providing Services to customers;

3.6.14. providing employee references;

3.6.15. registering employees as intermediaries or licensees with statutory authorities / institutions including tax authorities for purposes directly related or associated to the employment;

3.6.16. monitoring compliance with regulatory requirements and internal governance, policies, procedures, audit responsibilities, guidelines or rules of the Company;

3.6.17. complying with the obligations, requirements or arrangements for disclosing and using data that apply to the Company or any of its branches or that it is expected to comply according to:

(a) any law binding or applying to it within or outside the jurisdictions in which the Company operates existing currently and in the future; or

(b) any guidelines or guidance given or issued by any legal, regulatory, governmental, tax, law enforcement or other authorities, or self-regulatory or industry bodies or associations of financial services providers within or outside the jurisdictions in which the Company operates existing currently and in the future;

3.6.18. preventing, detecting or conducting investigation regarding any suspicious fraud cases, misconduct (e.g. fake sick leave), or criminal activities, including capturing images through CCTV and monitoring the use of facilities, network, premises, information, documents, computers, laptops, phones and other devices provided by the Company (for example, logon times and file access) and content (for example, copies of emails sent, types and levels of internet use such as downloading activity and access/attempted access to inappropriate, prohibited or blocked websites, inbound and outbound email activity, including emails sent externally, monitoring of telephone trends including content stored or transmitted through apps on the mobile phone, location information, and general usage data, logs of systems and user activity and external attempts to hack the Company's network or introduce viruses);

3.6.19. for human resource management or purposes relating thereto, including grievance procedures, disciplinary procedures and managing whistle blowing reports; and

3.6.20. any other purposes relating thereto and as notified from time to time.

3.7. Subject to paragraph 9 below, the purposes listed in paragraphs 3.5 and 3.6 may continue to apply even in situations where the customer's relationship with the Company has been terminated or altered in anyway, for a reasonable period thereafter (including, where applicable, a period to enable the Company to enforce their rights under any contract with the customer).

## 4. SECURITY OF PERSONAL DATA

4.1. It is the policy of the Company to ensure an appropriate level of protection for personal data in order to prevent unauthorised or accidental access, processing, erasure, loss or use of that data, commensurate with the sensitivity of the data and the harm that would be caused by occurrence of any of the aforesaid events.

4.2. It is the practice of the Company to achieve appropriate levels of security protection by restricting physical access to and processing of data by providing secure storage facilities, and incorporating security measures into equipment in which data is held.

4.3. Measures are taken to ensure the integrity, prudence and competence of persons having access to personal data and the access to the personal data is granted on a need-to-know basis only.

4.4. Personal data is only transmitted by secured means to prevent unauthorised or accidental access. If the Company engages a data processor / intermediary to process personal data on the Company's behalf, the Company would adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

5. ACCURACY OF PERSONAL DATA

5.1. It is the policy of the Company to ensure that all practicable steps have been taken to maintain the accuracy of all personal data collected and processed by the Company having regard to the purpose for which the personal data is or is to be used.

5.2. Whilst the Company has in place appropriate procedures to regularly check and update personal data that it holds, the Company also relies on customers to correct and update personal data and particulars as and when such information changes and in accordance with the Company's Website Terms of Service (www.getsprout.co/legal/tos), and the terms of the Master Service Agreement (www.getsprout.co/legal/msa). In so far as personal data held by the Company consists of statements of opinion, all reasonably practicable steps are taken to ensure that any facts cited in support of such statements of opinion are correct.

6. COLLECTION OF PERSONAL DATA

6.1. When collecting personal data, the Company will satisfy itself that the purposes for which the data is collected are lawful and directly related to the Company's functions or activities. The manner of collection is lawful and fair in the circumstances and the personal data collected is necessary but not excessive for the purposes for which it is collected.

6.2. In the course of collecting personal data directly from the individuals concerned, the Company will provide the individuals concerned with a Personal Information Collection Statement informing them of the purpose of collection, classes of persons to whom the data may be transferred, their rights to access and correct the data, and other relevant information. Practicable steps will be taken by the Company to ensure that the individuals concerned are informed of whether their consent is necessary for the Company's provision of the Services and, if necessary, the consequences for them if they do not consent.

6.3. In the course of collecting personal data indirectly (e.g., through the individual's employer), the Company will also provide the provider of personal data with a Personal Information Collection Statement informing them of the purpose of collection, classes of persons to whom the data may be transferred, the rights of individuals to access and correct the data, and other relevant information.

6.4. Prior to using any personal data from the public domain, due regards will be given by the Company to observe the original purposes of making the personal data available in the public domain (such as the purpose of establishing the public register in the enabling legislation). The restrictions, if any, imposed by the original data users on further uses and the reasonable expectation of personal data privacy of the individuals concerned will be observed by the Company.

6.5. In relation to the collection of personal data online, the following practices are adopted:

6.5.1. Online Security
The Company will follow strict standards of security and confidentiality to protect any information provided to the Company online. End to end encryption technologies are employed for sensitive data transmission on the Internet to protect individuals' privacy.

6.5.2. Online Correction
Personal data provided to the Company through an online facility, once submitted, may not be facilitated to be deleted, corrected or updated online. If deletion, correction and updates are not allowed online, users should approach the Company, relevant departments or branches for assistance.

6.5.3. Online Retention
Personal data collected online will be transferred to the relevant departments with the Company for processing. Personal data will be retained in the Company's internet system database normally for a period of no longer than 6 months unless such personal data is necessary for the Company's provision of Services to customers. Personal data transferred to the relevant departments will be retained for such duration to enable the Company to provide Services.

6.6. Use of Cookies, Tags and Web Logs etc.

6.6.1. Cookies are small pieces of data transmitted from a web server to a web browser. Cookie data is stored on a local hard drive such that the web server can later read back the Cookie data from a web browser. This is useful for allowing a website to maintain information on a particular user.

6.6.2. Cookies are designed to be read only by the website that provides them. Cookies cannot be used to obtain data from a user's hard drive, user's email address or user's sensitive information.

6.6.3. The Company uses cookies, tags and web logs to identify users' web browser for the following purposes:

- (a) Session Identifier
  The Company will not store user's sensitive information in Cookies. Once a session is established, all the communications will use the Cookies to identify a user.

- (b) Analytical Tracking
  Users' visit to the Company's online platforms and social networks (including but not limited to the Company's websites, mobile applications and LinkedIn and Twitter will be recorded for analysis and information may be collected through technologies such as cookies, tags and web logs, etc. The information collected is anonymous research data and no personally identifiable information is collected. The Company mainly collects the information to understand more about the Company's users including user demographics, interests and usage patterns, and to improve the effectiveness of the Company's online marketing.

6.6.4. The information may be transferred to or collected by third parties on the Company's behalf (for example, providers of external service like web traffic tracking and reporting, online advertisement serving) for the above use. The information would not be further transferred to other parties by the third parties engaged by the Company. The information collected is anonymous research data and no personally identifiable information is collected or shared by the third parties.

6.6.5. Most web browsers are initially set up to accept Cookies. Users can choose to "not accept" cookies by changing the settings on the web browsers but this may disable the access to or the user experience of the Company's platform and its features. Social networks may also not work properly. The Company will retain the collected information for as long as is necessary to fulfil the original or directly related purpose

for which it was collected and to satisfy any applicable statutory, regulatory or contractual requirements.

6.6.6. The information collected through technologies such as Cookies, tags and web logs etc. will not be kept longer than is necessary for the fulfilment of the purpose for which such data is or is to be used, or for legal or business purposes and will usually be retained for a period of no longer than 3 years, except where required by law.

6.7. The Company may install closed circuit television ("CCTV") (with recording mode) systems at its premises primarily for general security purposes to protect the safety of customers, visitors and its staff, business assets, intellectual property or other proprietary rights. Access to and use of the CCTV records will be granted to authorised personnel only. The Company may disclose the CCTV records to third parties including regulatory authorities and law enforcement agencies where it is necessary in order for it to respond to any legal processes or to investigate any incidents or complaints, etc.

6.8. Subject to the aforesaid, all CCTV records will be erased permanently and securely according to the Company's policies and guidelines. Any physical matter such as tapes, discs, still photographs and hardcopy prints will be disposed of as confidential waste. The security measures that apply to the CCTV records will be consistent with this Statement.

6.9. The Company may monitor the use of computers, laptops, phones and other devices provided by the Company for legitimate business purposes only and according to the Company's policies and guidelines. By using such devices provided by the Company, employees are deemed to have consented to the collection, use and disclosure of their personal data for such purpose.

## 7. DATA ACCESS REQUESTS AND DATA CORRECTION REQUESTS

7.1. It is the policy of the Company to comply with and process all data access requests ("DARs") and data correction requests ("DCRs") in accordance with the provisions of relevant laws of the jurisdictions in which the Company operates, and for all staff tasked with the responsibility to be familiar with the requirements for assisting individuals to make such requests.

7.2. The Company may, subject to applicable laws and regulations, impose a fee for complying with a DAR. The Company is only allowed to charge a DAR requestor for the costs which are directly related to and necessary for complying with a DAR. A written estimate of the fee shall be provided to the individual making the DAR request. If a person making a DAR requests for an additional copy of the personal data that the Company has previously supplied pursuant to an earlier DAR, the Bank may charge a fee to cover the full administrative and other costs incurred in supplying that additional copy.

7.3. DARs and DCRs to the Company may be addressed to the Company's Group Data Protection Officer ("GDPO") or any other person as specifically advised. If the Company is unable to accede to the individual's DAR and/or DCR, the Company shall inform the individual of the reason why the Company was unable to do so (except where the Company is not required or prohibited to do so under any applicable law).

## 8. RETENTION OF PERSONAL DATA

8.1. The Company takes all practicable steps to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose for which such data is or is to be used, or for legal or business purposes. The Company usually holds data relating to the customer(s) and employee(s) for a period of 7 years or such other period as prescribed by applicable laws and regulations after closure of account, termination of service or cessation of employment.

8.2. Regarding personal data collected from job applicants, unless there is subsisting reason that the Company is obliged to retain the data for a longer period (such as a period as prescribed by applicable laws and regulations), the Company will only hold the data of unsuccessful

applicants as long as it is necessary for business or legal purposes, usually for a period up to 2 years from the date of rejecting the applicants.

8.3. If the Company engages a data processor to process personal data on the Company's behalf, the Company would adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

## 9. TRANSFER OF PERSONAL DATA OVERSEAS

9.1. Where the Company transfers personal data overseas, the Company will take steps to ensure that the recipients of such personal data are bound by legally enforceable obligations to keep the personal data confidential, to use the personal data only for purposes that are approved by the Company and to cease to retain the personal data once such purposes are fulfilled.

## 10. OTHER PRACTICES

10.1. The Company will keep this Statement under regular review.

10.2. The following are maintained by the Company to ensure compliance with the Ordinance:

10.2.1. Log books as required under relevant laws; and

10.2.2. Internal policies and guidelines for observance by staff of the Company.

## 11. APPOINTMENT OF DATA PROTECTION OFFICER

11.1. The GDPO has been appointed by the Company to co-ordinate and oversee compliance with applicable laws and the personal data protection policies of the Company.

11.2. The contact details of the GDPO are as follows: api@stakingrewards.com