Personal Information Protection Notice for EU Contractors

1. Introduction

BetterUp, Inc. and its subsidiaries and/or affiliates ("Company", "we" or "our") operate in many different countries. Some of these countries have laws related to the collection, use, transfer and disclosure of the personal information of individuals, including employees. We take these obligations very seriously and are committed to protecting the privacy of our current and former employees.

The purpose of this Contractor Personal Information Protection Notice for EU Employees ("Notice") is to give contractors who are based in the European Union (including contractors based in the UK after the UK leaves the European Union, "EU Contractors") information about: what personal information we collect; how we collect, use and disclose that information and the legal grounds for us doing this; and our rights in respect of your personal information.

The Company is the data controller of your personal information and is responsible for how your personal information is processed.

This Notice does not form part of your services contract and may be updated at any time. We will provide you with a revised Notice if we make any substantial updates. It is important you read this Notice, so that you are aware of how and why we are using your personal information.

2. What Information We Collect About EU Contractors

We may collect and process information about EU Contractors before, during or after completion of the services with the Company as detailed in this notice. We refer to such information in this Notice as "EU Personal Information." We may collect the following EU Personal Information as applicable:

- **Personal Details:** Name, identification number, date of birth, work and home contact details (email, phone numbers, physical address) languages(s) spoken, gender, date of birth, national identification number, social security number, driver's license number, marital/civil partnership status, disability status, emergency contact information and photograph;
- **Documentation Required under Immigration Laws:** Citizenship and passport data, details of residency or work permit;
- **Compensation and Payroll:** Fee schedule, compensation type, currency, pay frequency, effective date of current compensation, banking details, working time records (including hours worked and tasks completed), pay data and termination date;
- **Talent Management Information:** Details contained in letters of application and resume/CV (previous employment background, education history, professional qualifications, language and other relevant skills, certification, certification expiration dates), information necessary to complete a background check, details on performance management ratings, development programs planned and attended, e-learning programs, performance and development reviews, willingness to relocate, and information used to populate employee biographies;
- **System and Application Data:** Information required to access company systems and applications such as System ID, LAN ID, email account, instant messaging account, mainframe ID, previous employee ID, previous manager employee ID, system passwords, employee status reason, branch state, country code, previous company details, previous branch details, and previous department details, and electronic content produced by you using Company systems; and

- **Sensitive Information:** health/medical information, trade union membership information, information and religion, race and ethnicity, and criminal convictions data if legally permissible.

3. Sources of EU Personal Information

We collect EU Personal Information from the following sources:

- **EU Contractors:** in person, online, by telephone, or in written correspondence and forms;
- **Third-party websites:** where you can apply for jobs at the Company or take advantage of services made available to employees;
- **Previous employers:** in the form of employment references;
- **Background and credit check vendors**: as part of the recruitment process;
- **Employment agencies and recruiters**; and
- **Providers of sanctions, prohibited persons lists, and "politically exposed persons" screening lists**

4. How we use and disclose EU Personal Information

Legal Basis for Processing

We will only use EU Personal Information when the law allows us to. Most commonly, we will use your EU Personal Information in the following circumstances:

- Where it is necessary to perform obligations or exercise rights under your employment contract or contractor agreement;
- Where it is necessary to comply with a legal obligation on us (including, in respect of Sensitive Information, obligations under employment law); and
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. For example, the Company has a legitimate interest in the processing and group-wide transfer of EU Personal Information for group company internal business purposes, including to manage the centralization of data processing activities, to design efficient and workable business processes, to allow cross-company teams to work together and to make business processes more efficient and cost effective.

We may also use your EU Personal Information in the following situations, which are likely to be rare:

- Where it is necessary to protect your (or someone else's) vital interests (and, in the case of Sensitive Information, where you are incapable of consenting);
- Where it is necessary for us to defend, prosecute or make a claim related to your employment; and
- In the case of Sensitive Information, where you have made the information public

In particular, we may use your Sensitive Information, such as health/medical information, in order to accommodate a disability or illness and to provide benefits, your diversity-related EU Personal Information (such as race or ethnicity) in order to comply with legal obligations relating to diversity and anti-discrimination, and your criminal conviction data only where it is appropriate (given your role) and we are legally able to do so in order to comply with regulatory requirements, where applicable.

Purposes of Processing

We process EU Personal Information for the following purposes**:**

- **Managing Workforce:** Managing work activities and personnel generally, including recruitment, appraisals, performance management, promotions and succession planning, rehiring, administering salary, and payment administration and reviews, wages and other awards such as stock options, stock grants and bonuses, healthcare, pensions and savings plans, training, leave, managing sickness leave, promotions, transfers, secondments, honouring other contractual benefits, providing employment references, loans, performing workforce analysis and planning, performing employee surveys, performing background checks, managing disciplinary matters, grievances and terminations, reviewing employment decisions, making business travel arrangements, managing business expenses and reimbursements, planning and monitoring of training requirements and career development activities and skills, and creating and maintaining one or more internal employee directories;
- **Communications and Emergencies:** Facilitating communication with you, ensuring business continuity, providing references, protecting the health and safety of employees and others, safeguarding IT infrastructure, office equipment and other property, facilitating communication with your nominated contacts in an emergency;
- **Business Operations:** Operating and managing the IT and communications systems, managing product and service development, improving products and services, managing company assets, allocating company assets and human resources, strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, maintaining records relating to business activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, sales, re-organisations or disposals and integration with purchaser; and
- **Compliance:** Complying with legal and other requirements, such as income tax and national insurance deductions, record-keeping and reporting obligations, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claims, conducting investigations and complying with internal policies and procedures

There may be more than one purpose that justifies our use of your EU Personal Information in any particular circumstance.

We will only use your EU Personal Information for the purposes for which we collected it or for another reason and that is reasonably compatible with the original purpose. If we need to use your EU Personal Information for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

If you fail to provide certain EU Personal Information when requested, we may not be able to perform your services contract (e.g., by paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers or the security of the data we process).

<u>Disclosures to third parties</u>

We share EU Personal Information with the following unaffiliated third parties**:**

- **Professional Advisors:** Accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors in all of the countries in which the Company operates;

- **Service Providers:** Companies that provide products and services to the Company such as payroll, pension or equity scheme, benefits providers, human resources services, occupational health services, performance management, training, expense management, IT systems suppliers and support and background check providers; third parties assisting with equity compensation programs, credit card companies, medical or health practitioners, trade bodies and associations, claims handlers and loss adjusters, and hosting service providers;
- **Public and Governmental Authorities:** Entities that regulate or have jurisdiction over the Company such as regulatory authorities, public bodies, and judicial bodies, including to meet national security or law enforcement requirements;
- **Third Parties in Corporate Transactions:** in connection with any proposed or actual reorganisation, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of the Company's business, assets or stock (including in connection with any bankruptcy or similar proceedings); and
- **Future Employers and their Vendors**

5. Transfer of Personal Information

The Company may disclose EU Personal Information throughout the world to fulfil the purposes described above. This may include transferring EU Personal Information to other countries (including countries other than where an EU Employee is based and located outside the European Economic Area ("EEA")) that have different data protection regimes and which are not deemed to provide an adequate level of protection for EU Personal Information. To ensure that your EU Personal Information is sufficiently protected when transferred outside the EEA the Company has put in place the following measure: a data transfer agreement incorporating the EU's standard contractual clauses. Further information regarding the Company's protective measure is available from the Company's DPO (defined below).

6. Data Security

The Company will take appropriate measures to protect EU Personal Information that are consistent with applicable privacy and data security laws and regulations, including requiring service providers to use appropriate measures to protect the confidentiality and security of EU Personal Information.

Access to EU Personal Information within the Company will be limited to those who have a need to know the information for the purposes described above, and may include your managers and their designees, personnel in HR, IT, Compliance, Legal, Finance and Accounting and Internal Audit. All personnel will generally have access to EU Employees' business contact information such as name, position, telephone number, postal address and email address.

The Company has put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach of your EU Personal Information when we are legally required to do so.

7. Data Retention

The Company's retention periods for EU Personal Information are based on business needs and legal requirements. We retain EU Personal Information for as long as is necessary for the processing

purpose(s) for which the information was collected, as set out in this Notice, and any other permissible, related purposes. For example, we may retain certain information to comply with regulatory requirements regarding the retention of such data, or in the event a litigation hold is imposed. When EU Personal Information is no longer needed, we either irreversibly anonymize the data (and we may further retain and use the anonymized information) or securely destroy the data.

8. Data Accuracy

The Company will take reasonable steps to ensure that the EU Personal Information processed is reliable for its intended use and is accurate and complete for carrying out the purposes described in this Notice.

9. Automated Decisions

The Company does not envisage that you will be subject to decisions that will have a significant impact on you based solely on automated decision-making. The Company will notify you in writing if this position changes.

10. Your Rights

You have the right, in certain circumstances, to object to the processing of your EU Personal Information. You can exercise this right by contacting the Company's care team at support@betterup.co.

You also have the right, in certain circumstances, to access your EU Personal Information, to correct inaccurate EU Personal Information, to have your EU Personal Information erased, to restrict the processing of your EU Personal Information, to receive the EU Personal Information you have provided to the Company in a structured, commonly used and machine-readable format for onward transmission, and to object to automated decision-making. If you wish to exercise any of these rights please contact BetterUp at support@betterup.co. Please note that certain EU Personal Information may be exempt from such access, correction, erasure, restriction and portability requests in accordance with applicable data protection laws or other laws and regulations.

You also can file a complaint with your local data protection supervisory authority. Please contact the Company's Customer Care Team at support@betterup.co for details of the relevant authority.

11. Your Obligations

You should keep your EU Personal Information up to date and inform us of any significant changes to your EU Personal Information. You further agree to follow applicable law and the Company's policies, standards and procedures that are brought to your attention when handling any EU Personal Information to which you have access in the course of your relationship with the Company. In particular, you will not access or use any EU Personal Information for any purpose other than in connection with and to the extent necessary for your work with the Company. You understand that these obligations continue to exist after termination of your relationship with the Company.

12. Questions or Complaints

The Company has a dedicated Data Protection Officer to oversee compliance with this Notice. For any questions or complaints regarding this Notice or the Company's privacy practices, please contact the

Data Protection Officer by phone at +1 (415) 992-6160 or toll free +1 (844) 303-9595, by email at compliance@betterup.co, or in writing to:

BetterUp, Inc.
1200 Folsom St.
San Francisco, CA 94103
United States