Effective Date: May 2021

Responsible Official: Executive Director

EU Employee Data Protection Notice

Green Mountain Higher Education Consortium, Inc., has prepared this Employee data protection notice (including, where applicable, any country-specific schedules) (the "Notice") to describe its practices regarding the collection, us, storage, transfer, and other processing of personal information – individually identifiable information – about Employees from the European Union. The Consortium is the controller responsible for the personal information that we collect, and process as described in this Notice. For the purposes of this Notice, "Employee" means:

- Past and present employees;
- Past and present consultants, independent contractors, and agents;
- Job applicant;
- Past and present temporary employees;
- Retirees; and
- Past and present directors and officers

1 Information We Collect

We may collect your personal information from a variety of sources, including information we collect from you directly (e.g., when you apply for a job, during your employment, following termination of employment, etc.), and information we collect about you from other sources (where permitted by law).

Certain personal information is required as a consequence of the contractual relationship we have with you when we employ you, the enable us to carry out our contractual obligations to you. Failure to provide this information may prevent or delay the fulfillment of these obligations.

1.1 Information We Collect Directly from You

The categories of information that we may collect directly from you include the following:

1. personal details (e.g., name, age, date of birth);
2. contact details (e.g., phone number, email address, postal address);
3. family contact personal details (e.g., emergency contact details);
4. other information about you and your family (e.g., gender, marital status, legal and/or work permit status within the U.S., family status, dietary requirements, hobbies);
5. educational and career background (e.g., your resume);
6. employment details (e.g., employee number, PPS number, career planning reports, annual review reports, job start date, job end date);

7. job performance details (e.g., performance evaluations);
8. employment and salary administration (e.g., salary amount, bank details, benefit details, tax certificate details);
9. other relevant date in respect to your job application or employment with us (e.g., job location, working conditions, special leave, special needs, holidays, etc.);
10. data regarding special agreements (e.g., professional development allowances, health insurance allowances, etc.); and
11. your UP address and activity when using computing resources in the Consortium's internal network, or when using the Consortium's online services (e.g., Oracle).
12. Photograph(s)

1.2 Information We Collect from Other Sources

The following are examples of the categories of information we may collect from other sources:

1. personal details (e.g., name, age, date of birth);
2. contact details (e.g., phone number, email address, postal address);
3. educational and career background (e.g., references from former employers, checks on validity of academic credentials);
4. job performance details (e.g., performance evaluations);
5. other information about you and your family (e.g., gender, marital status, family status); and
6. employment administration data (e.g., tax payment details, payroll details, pension details, group life insurance underwriting details).

2 How We Use Your Personal Information and the Basis on Which We Use It

2.1 Use of Your Personal Information

We use your personal information in relation to your job application and (current or past) employment with us, to:

1. carry out our obligations to you under your terms of employment;
2. exercise our rights under your terms of employment;
3. provide any services you request from us;
4. to keep our records accurate and up-to-date; and
5. comply with legal obligations to which are subject.

2.2 Use of Your Personal Information

We must have a legal basis to process your personal information. In most cases the legal basis will be one of the following:

1. to fulfill our contractual obligations to you, for example to ensure that your salary is paid correctly, and for ensuring you have appropriate access to our premises;
2. to meet our legal obligations to you as your employer, for example health and safety obligations while you are on our premises; or to a third party (e.g., tax authorities); and,

3. to meet our legitimate interests, for example to ensure that we can provide you with any services, for example HR services from us, and that our records are kept up to date and accurate.
4. While the Consortium does not generally monitor or limit content of information transmitted and stored on its network, it reserves the right to access and review such information when necessary or in response to a judicial or governmental request, requirement or order.

2.3 Special Categories of Personal Information

We collect and process certain special categories of personal information about Employees where necessary and in compliance with applicable local data protection laws. In particular, the Consortium processes health data, union membership (if applicable) and racial and/or ethnic data, as required and to the extent permitted under local laws to carry out its obligations in the field of employment, health and safety, social security, and social obligations law and, where necessary, for the establishment or defense of legal claims.

2.4 Change of Purpose

We will only use your personal information for the purposes (see 2.1 to 2.3 above) for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

3 How We Store Personal Information and Who Can Access It

The Consortium maintains a digital record of each Employee's personal information. This automated record contains most of the data held in the Employee's personnel file. Additionally, the Consortium maintains personal information in various human resources applications, including applications for payroll, benefits, talent management and performance management. The Consortium may maintain individual hard-copy personnel files. The Consortium maintains these files in a secure environment.

Access to personal information is restricted to those individuals who need such access for the purposes listed above or where required by law, including Consortium administrative staff, members of the Consortium People Services Department, the managers in the Employee's department or division, and to authorized representatives of the Consortium's internal control functions such as Finance and Legal. Access may also be granted on a strict need-to-know basis to other managers in the Consortium where relevant if the Employee is being considered for an alternative job opportunity, or if a new manager appointed in the line of business needs to review files. All Employees, including managers, are bound by the requirement of this Notice.

4 Your Rights Over Your Personal Information

Please let us know if any of the personal information that we hold about you changes so that we can correct and update the information on our systems.

You can view, delete, correct, or update the personal information you provide to us by making a written request to the Consortium's Data Protection Manager at dataprivacy@gmhec.org.

In certain circumstances you may object to specific processing activities, require us to restrict how we process your personal information and ask us to share your personal information in a usable format with another company. Where you have given your consent to a particular type of processing, you may withdraw that consent at any time.

To exercise any of the above rights, please contact us using the contact details set out below.

5 Information Sharing

In general, we do not share your personal information with third parties (other than service providers acting on our behalf) unless we have a lawful basis for doing so.

We rely on third-party service providers to perform a variety of services on our behalf, which may mean that we have to share your personal information with these third parties. When we share your personal information in this way, we put in place appropriate measures to make sure that our service providers keep your personal information secure.

Other situations in which we may disclose your personal information to a third party, are:

1. in the course of a sale or an acquisition of the Consortium;
2. where permitted by law, to protect and defend our rights and property; and
3. where required by law, and/or public authorities.

6 Information Security

We have implemented generally accepted standards of technology and operational security to protect personal information from loss, misuse, alteration, or destruction. We require Employees and principals to keep personal information confidential and provide access to this information only to authorized personnel.

We will retain your personal information in accordance with our data retention policy which sets out data retention periods required or permitted by applicable law.

7 Information Transfer

Your personal information may be transferred to, stored, and processed in a country other than the one in which it was provided. When we do so, we transfer the information in compliance with applicable data protection laws. Where the transfer is to a country outside the EEA, we use one of the following mechanisms to ensure that the appropriate level of data protection is in place:

1. If the organization or service provider to which we are transferring is based in the U.S. and has signed up to the EU-U.S. Privacy Shield, then we are assured by that mechanism that the

appropriate technical and organization measures have been put in place to address data protection.

2. If they are outside the EEA, the country in question is not covered by an Adequacy decision by the EU Commission and, in the case of the U.S., are not covered by the Privacy Shield, then we rely on the European Union Standard Contractual Clauses which stipulate that the appropriate technical and organizational measures be put in place to address the protection of the data transferred. If you wish to see a copy of the relevant mechanism that we use to transfer your personal information, please contact us using the contact details set out below.

8 Dependent's Privacy

We may process personal information of your family members, including your children. When we do so, we will do so in compliance with data protection laws as they apply to children.

9 Contact Us

If you have questions or concerns regarding the way in which your personal information has been used, please contact the Consortium Data Protection Manager at dataprivacy@gmhec.org.

We are committed to working with you to obtain a fair resolution of any complaint or concern about privacy. If, however, you believe that we have not been able to assist with your complaint or concern, you have the right to make a complaint to the Data Protection Commission in the appropriate jurisdiction.

10 Changes to the Privacy Notice

You may request a copy of this privacy notice from us using the contact details set out above. We may modify or update this privacy notice from time to time. You will be able to see when we last updated the privacy notice because we will include a revision date. Changes and additions to this privacy notice are effective from the date on which they are posted. Please review this privacy notice from time to time to check whether we have made any changes to the way in which we use your personal information.