Pantheon Platform UK, Limited

Employee and Applicant Privacy Policy

Last Updated June __, 2022

This Employee and Applicant Privacy Policy ("Privacy Policy") addresses how Pantheon Systems, Inc. and its affiliates, including Pantheon Platform UK, Limited ("we," "our," "Pantheon") handles information we gather from employees and applicants for a position at Pantheon in the United Kingdom. Questions regarding this statement should be e-mailed to **privacy@pantheon.io**. This Privacy Policy describes the ways we collect, use and share employee and applicant information.

This Privacy Policy describes the types of personal data we may collect from you when you visit our website, apply for a job or become an employee, as well as the way we use and process that personal information.

Please read this Privacy Policy so that you are aware of how and why we use your personal data. This Privacy Policy may change from time to time, as reflected in the revision date above.

Pantheon is the data controller, as defined under the EU General Data Protection Regulation (EU) 2016/679 ("GDPR") as adopted by the UK, dictating the processing of your personal data by Pantheon and its various service providers, such as service providers who provide benefits to you if you are an employee.

Information Gathered

Personal information or personal data means any information about an individual from which that person can be identified. It does not include data where the information that identifies a specific individual has benn removed, such as pseudonymized or anonymized data.

We may collect, store, use and transfer different kinds of personal information about you, which information, and the circumstances of its collection, are grouped below:

- **Applicant/Employee:** We collect certain information automatically from website visitors using cookies and similar technologies, including information from third parties. For more information, see our Cookie Policy at https://pantheon.io/pantheon-cookies.
- **Applicant/Employee**: We collect, store, and process information that you provide to us when you communicate with us.
- **Applicant/Employee**: We collect, store, and process information that you provide to us when you apply for a position with Pantheon. Such information may include name, address, email address, telephone number and other contact information, resume or CV, cover letter, previous and/or relevant work experience or other experiences, education, transcript, or other information that the job applicant may provide to us in support of an application and/or recruitment process. We may also obtain information from interviews and phone-screening. We may also collect details about the type of employment the applicant may be looking for, current and/or desired salary and other terms related to compensation and benefits packages, willingness to relocate, or other job preferences; details of how the applicant heard about the job opening; any sensitive and/or demographic information obtained during the application or recruitment process such as gender, age, information about citizenship and/or nationality, medical or health information and/or your racial or ethnic origin; reference information and/or information received from background checks, including criminal background checks, where applicable, as well as information provided by third-parties; and information related to any assessment you may take as part of the interview screening process.

This information is retained while you are an employee of Pantheon and is deleted subject to Data Privacy guidelines.

- **Employee**: We collect, store and process information necessary to enable us to provide your compensation or pay an invoice, including your name, address, government identification number, salary information, and bank account details. If you are an employee, we also collect, store and process information regarding your tax and retirement savings account plan elections.
- **Employee**: We collect, store and process information necessary for us to provide you with offered benefits, including various insurance programs and other benefits, and may also collect store, and process the following information for any family member or beneficiary listed on your benefits, including benefit selections, medical information, marital status (and, incidentally, sexual orientation), beneficiaries, other covered parties and their age, gender and relationship to you. We also collect, store and process information concerning your job performance and reviews, compensation history within Pantheon, job titles and promotions, dates of employment, training records, leave entitlements, disability-related accommodation requests, updated contact information, use of Pantheon IT systems, employee identification number, photographs, signatures, video images.

Special Categories of Personal Data. We may collect and process Special Categories of Personal Data, which is information that reveals racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

Aggregate Data.We also collect and use certain Aggregate Data, which has been anonymized, such as statistical data regarding race, age and gender, for lawful purposes, such as diversity reporting. As noted above, this type of data is not considered personal information subject to privacy laws and regulations.

Information Use

We only use your personal data when the law allows us to. See Legal Basis for Processing, below.

Recruitment. Pantheon stores and processes information provided by job applicants for the purposes of carrying out application and recruitment processes. Pantheon uses applicant information to assess skills and qualifications against the applicable job opportunity; verify information and conduct reference checks; and comply with applicable laws, regulations, legal processes, or enforceable governmental requests.

Employment: Pantheon stores and processes information provided by an employee for purposes of carrying out the employment relationship, including the provision of benefits and compensation, onboarding, workflow management, talent management and succession planning, monitoring and enforcing compliance with Pantheon policies and procedures, safety and security monitoring, performing internal or external audits, investigating and enforcing disciplinary measures, and addressing legal disputes. We may also ask for consent for special conditions pertaining to Work from Home or other Remote Work arrangements.

Sharing of Information

Pantheon will not copy, distribute, or otherwise share any applicant or employee data except as set out in this Privacy Policy. Pantheon may share applicant or employee data in the following ways, subject to the existence of a legal basis for the sharing and processing of such information:

- **Group Companies**:From time to time, Pantheon may disclose your personal information to one of our Group Companies for business purposes, including sannouncing corporate developments, sending invitations to Company events, and announcing new benefit and other programs.
- **Service providers:** From time to time, we may disclose your personal information to organizations that perform services for Pantheon, such as processing job applications, conducting background checks, providing benefits, enabling payment and/or reimbursement, providing consulting services regarding business operations, conducting investigative or providing legal services, and similar services. We will share with these companies only the personal information they need to provide the

services. These service providers will be required to agree to use the personal information of applicants, employees solely for the purpose of providing the services, under Pantheon's instructions, to keep that information secure, and otherwise comply with all applicable data privacy laws and regulations.

- **Potential acquirers of Pantheon's business:** If the stock or assets of Pantheon, its subsidiaries, its joint ventures or any combination of such are acquired by another entity, some or all of the personal information of applicants, employees may be provided to such a successor. In such a case, the successor will be instructed to handle the personal information in the same manner as provided in this Employee Privacy Policy.
- **Law enforcement:** We may be required in certain circumstances to disclose personal information in response to a lawful request by public authorities, the courts, law enforcement, or to comply with national security requirements. To the extent allowed by law, we will notify you before or in conjunction with a required disclosure. To the extent allowed y law, we will notify you before disclosure is made, as well as seek to object to or limit the scope of the request
- **Consent:** We may disclose your personal information to third parties where we have your consent to do so, except as otherwise prohibited by law.

Legal Basis for Processing

We will use your personal information when we are performing contractual obligations, where it is necessary for our legitimate interest and your interests and fundamental rights do not override our interest, or when necessary to comply with a legal obligation.

If we ask you to provide personal information to comply with a legal requirement or to contact you, we will make this clear at the relevant time and advise you whether the provision of your personal information is mandatory (as well as the consequences if you do not provide your personal information).

If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, please contact us as indicated above.

Security

Pantheon uses appropriate administrative, technical, organizational, and physical security measures to protect applicants' and employees' personal information against accidental or unlawful destruction, loss, and alteration, and against unauthorized disclosure and access. We use standard industry practices to protect personal information, including firewalls, SSL encryption, system redundancies, and co-location at a 24/7 secured, controlled environment.

We have procedures in place to address any suspected data breach and will notify you and the applicable regulator of a breach whenever we are legally required to do so.

Data Transfers

Employees' and applicants' personal information may be transferred to, and processed in, countries other than the country in which they reside. Whenever we transfer your personal data outside of the UK or EEA, as the case may be, we ensure that a similar degree of protection is afforded to it by having at least one of the following safeguards in place: (i) the country to which we transfer your personal data has been deemed to provide an adequate level of protection for personal data, or (ii) we have in place specific contracts approved for use in the UK and EEA (the Standard Contractual Clauses approved for use by the UK and the European Commission). For more information about how we transfer personal information of applicants and employees, please contact us at privacy@pantheon.io.

You may direct inquiries or complaints concerning Pantheon's processing of personal information to privacy@panthon.io. Pantheon will respond within the time limits prescribed by applicable law and, if applicable law does not address such time frame, within 30 days.

If you have an unresolved data privacy or data use concern that we have not addressed satisfactorily, please contact the Information

Commissions' Office (ICO), the United Kingdom regulator for data protection issues at www.ico.org.uk. We would, however, appreciate the chance

Accessing and Updating Contact Information

We encourage our applicants and employees to access, update and edit their contact information to keep the information current. Employees can access, correct or update their contact information by communicating with the People Team or using self-serve mechanisms within the tools supplied to employees. Applicants can also update their information by reaching out to the Pantheon recruiter or by using the automated tool labeled "Data Subject Request" located at the bottom of Pantheon's homepage at www.pantheon.io.

Your Data Protection Rights

You can exercise any one of the following data protection rights as may be available to you under applicable law by contacting us at privacy@pantheon.io. We will acknowledge and respond to your data protection rights requests promptly and in all cases no later than within 30 days unless required sooner under applicable law. You have the following data protection rights:

- You have the right to **access, correct, update or request deletion** of the personal information we collect about you. Please note that Pantheon may have a legal right or other obligation or a legitimate interest to maintain certain information about you, irrespective of your request for deletion.
- You have the right to **object to processing** of your personal information, ask us to **restrict processing** of your personal information or **request portability** of your personal information.
- If we have collected and processed your personal information with your consent, you can **withdraw your consent** at any time by contacting the People Team, the Pantheon recruiter you are working with, or by using the Data Subject Request portal at the bottom of Pantheon's homepage at www.pantheon.io. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal data conducted in reliance on lawful processing ground other than consent.
- You also have a right to **request erasure** of some of your personal information from our systems, again by contacting the People Team, your recruiter, or using the portal for Data Subject Requests at the bottom of our homepage. Asking for erasure may not affect the lawfulness of Pantheon's retention and continued processing of personal information where it has a legal obligation or other legal basis to maintain the data.
- Please refer to Data Privacy Regulations in your particular geographic location for specific rights that may be provided in addition to the general description above.

Importantly, you also have the **right to complaint to the data protection authority** about our collection and use of your personal information. For more information, please contact the ICO, as noted in the introduction and Statement of Purpose above, or your local data protection authority. Contact details for the data protection authorities in the European Economic Area are available at http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index.en.htm.

If you with to exercise any of the rights above, please use the "Data Subject Request" portal on the bottom of the first page of Pantheon's website, contact the People Team or your Pantheon recruiter. You may also send an email to privacy@pantheon.io or mail a request to Legal/Privacy, Pantheon Systems, Inc., 717 California Street, Floor 2, San Francisco, California 94108. You may also call Pantheon at +1-855-927-9387 and ask for the General Counsel.

Receive Notice of Changes

Pantheon reserves the right to change this Employee Privacy Policy from time to time as necessary to reflect changing legal, regulatory

or operational requirements. Pantheon will provide notification of the material changes to this Employee Privacy Policy through its website and announcements made to employees during regular Weekly Kick Off meetings and/or by email.

Data Retention

We retain personal information we collect from you where we have an ongoing legitimate business need to do so as part of your application, employment or engagement with us and to comply with applicable legal, tax and accounting requirements.

When we have no ongoing legitimate business need to process your personal information, we will either anonymise it, or, if this is ot possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible. Under no circumstances do we retain data without a legitimate business need for greater than two years, except as may be required by applicable law.

Pantheon Liability

Pantheon understands privacy is an imperative for many people and they seek out those employers that share these values. In accordance with the GDPR principles, Pantheon remains liable for any processing of peraonal data from the UK, EEA and Switzerland by third party agents acting on our behalf where such processing is inconsistent with the GDPR, unless Pantheon was not responsible for the event giving rise to any alleged damage.