

Gendered Intelligence Privacy Notice – Employees

What is the purpose of this document?

This document is part of our commitment to being transparent about how we collect and use your data. It explains what Gendered Intelligence (GI) does with your data, and addresses how we meet our obligations under the General Data Protection Regulation (GDPR) 2018 and the Data Protection Act 2018. It covers all GI employees, including individuals working on a freelance or contract basis, or through an agency. It also covers job applicants and former employees.

Definitions

‘Personal data’ means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

‘Special category data’ is regarded as more sensitive, and includes information about race; ethnic origin; politics; religion; trade union membership; genetics; health; sex life; or sexual orientation.

‘Processing’ means collecting, storing, using, amending, disclosing or destroying data.

Trans experiences are not explicitly named in the GDPR. However we believe the information that someone has, or is considering whether they have, a gender identity that does not align with the sex they were assigned at birth should be treated as personal data. This is directly analogous to the special category of sexual orientation, and we believe it is arguably covered within the special categories of genetics and health data.

What data do we collect and why?

Gendered Intelligence collects and processes data about you during and after your relationship with us in order to manage that relationship, meet our contractual obligations to you, and report to our funders and stakeholders. We aim to comply with guidance from the Information Commissioner’s Office (ICO), the independent body that upholds your information rights in the UK.

As a trans-led organisation, we understand that some of your gender-related data or name may be different in different contexts, such as home, in educational and other work place settings and elsewhere. We have to comply with the law and keep you safe, but we are always mindful of your situation, will only share data where it is absolutely necessary, and aim not to out you without your permission in any situation. If you have any concerns please talk to your line-manager or the named representative for data protection.

The table below lists the potential range of data we may collect from you. We will only collect the information that is relevant and required for the specific purpose, so we may not collect all items of data from everyone.

Data we process	What we use it for
Names, addresses, telephone numbers, email addresses, date of birth, legal gender	To meet our contractual requirements.
National Insurance number, Bank account details, employee ID	To pay you and arrange pension payments on your behalf.
Information on access requirements,	To enable us to provide appropriate support and ensure

health or medical conditions	compliance with health and safety. To enable us to make reasonable adjustments as required.
Passport or residency documentation	To confirm your right-to-work status
Criminal Offence data, and data required to obtain a Disclosure and Barring Service (DBS) Check, such as addresses for previous four years	To ensure we are meeting our safeguarding obligations and protecting our business interests.
References	To assess your suitability for working with us
Educational and training information, such as certificates or awards	To build a picture of your skills, experience and interests in order to assess your suitability for employment opportunities, and to support you through our staff appraisal system
Performance-related data, such as career history, objectives, skills, application form, contract of employment	To inform our staff appraisal process.
Job-related data, such as years of service, work location, annual leave, sickness or other absences	To inform our staff appraisal process and meet our contractual obligations
Next of kin or emergency contact details	To ensure your friends or family are informed rapidly in the event of an emergency.
Photos	For communication purposes on our website or other marketing materials e.g. Annual Report

How is your data collected?

We collect data through the application process, either directly from you or from third parties, such as the references you will be asked to provide, or the Disclosure and Barring Service. We will also collect personal data in the course of your employment with us.

How can Gendered Intelligence use the data I provide?

We have to have a valid reason to use your personal data. This is called the "lawful basis for processing".

- The lawful basis by which we process the majority of your data is Contract: we require the data in order to fulfil our contractual obligations to you.
- For job applicants, the lawful basis is Legitimate Interests: the information you have provided is necessary for us to assess your application.

When we process special category data we also need to confirm a Special Condition under Article 9 of the GDPR. Where this data is anonymised, for example when we use it for Equal Opportunity reporting, it is no longer considered to be Personal Data.

- We confirm that for the majority of your Special Category Data Special Condition (b) applies, which means we need the information to comply with our contractual obligations to you.
- Where you have provided health data, Special Condition (c) – Vital Interests – may also apply, as we require the correct information to provide medical support in the event of an emergency.

- Where you have provided data about your trans identity we have requested your Explicit Consent (Special Condition (a) under Article 9)

When we process criminal offence data we aim to comply with Article 10 of the GDPR.

We also process data for your emergency contacts; the lawful basis on which we do this is Legitimate Interests.

We will only use your data for the purposes 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 data 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, where this is required or permitted by law.

Who has access to your data?

Your information will be shared internally, including with your line manager, the CEO, and staff members responsible for HR, IT, health and safety.

We may share your data with third parties, in the following circumstances:

- To meet our contractual requirements such as payroll or pension payments
- If we are required to do so by a court order or the law
- If you request us to share information, for example for mortgage loans or employment references
- In life-threatening emergencies
- To obtain pre-employment references or DBS checks

We require third parties to respect the security of your data and treat it in accordance with the law. We only permit them to process your personal data for specified purposes and in accordance with our instructions

Your legal rights

As a data subject, you have a number of rights, details of which can be found at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

If you believe that Gendered Intelligence has not complied with your data protection rights, you can complain to the ICO (www.ico.org.uk/concerns).

Changes to this privacy notice

We may update this privacy notice to comply with changes in the law or to reflect improved processes at GI: if we make substantial changes we will provide you with a new privacy notice. We may also notify you in other ways from time to time about the processing of your personal information.

Queries and Further Information

Gendered Intelligence, c/o VAI, 200 Pentonville Road, London N1 9JP is the Data Controller.

Further information is available at www.genderedintelligence.co.uk/data where you can view GI's Data Protection Policy and related policies and procedures, for example, how we deal with Data Security Breaches; how you can view or amend your data (via a Subject Access Request); and how long we keep your data for.

Alternatively, please contact the person responsible for data protection: Jay Stewart, CEO, jay.stewart@genderedintelligence.co.uk

Document review process

Version: 1.0

Draft approved for circulation: May 2018

Board approval due: July 2018

Review due: July 2020