DATA PROTECTION FAQS

This document is intended to answer the most common questions our customers ask about why and how we process personal data.

1. Who are Insights?

We are a global learning and development company, headquartered in the UK. Insights Learning & Development Limited ("ILD") is the main contracting entity. ILD is registered with the UK Data Protection Authority, the Information Commissioners Office ("ICO") under number Z7145849.

For many years, ILD has been developing psychometric tools to help people understand themselves, others and make the most of relationships that affect them in the workplace. The core offering is a unique personal profile (the "Profile") that can be used as a baseline fora variety of further training from individual coaching to team effectiveness. Our services are used worldwide in personnel and organisational development.

ILD trains and accredits Insights Discovery Practitioners. These are self-employed trainers, consultants, or HR employees of a company. Once accredited by ILD, the Insights Discovery Practitioners have access to our online platform, where they can create and manage Profiles.

For more information about us see www.insights.com.

2. What data do we require?

The Insights Discovery methodology uses a simple and memorable four colour model to help people understand their personal style, their strengths and the value they bring to a team. We call these the colour energies. It's the unique mix of Fiery Red, Sunshine Yellow, Earth Green and Cool Blue energies, which determines how and why people behave the way they do.

To facilitate the creation of a Profile, Insights collects limited personal data about the learner such as name and email address.

Typically, an Accredited Practitioner sends an invitation link to our online evaluator questionnaire to the Profile recipients taking part in a workshop. The Profile recipients confirm that they agree to our privacy policy and then provide their name, gender, company email address and reference code in order to complete the evaluator questionnaire. Once completed, the Profile is then delivered to the Profile recipient and available to access on the Accredited Practitioner's Insights online account. Profiles are stored here so that the Accredited Practitioner can explain the Profile to the recipient in greater detail. Profiles

contain data that is relevant to the individual Profile recipient. However, the only identifying information contained within the Profile is the recipient's name. No sensitive data is contained within the Profiles we issue.

3. Are we a controller or a processor?

We are an independent data controller and not a processor.

Accredited Practitioners or consultants working on our behalf to deliver workshops collect data directly from individual Profile recipient. The resultant Profile is then provided directly to the recipient. No data is collected from the employer and the Profile is not routinely shared with employers by us. Profile recipients must accept our privacy policy before completing our evaluator questionnaire. This privacy policy explicitly states that we will not share Profiles with anyone other than the relevant Profile recipient and the Accredited Practitioner providing the training. Our Profiles are for the benefit of the individual Profile recipient completing the evaluator questionnaire. These are not completed on behalf of employers.

We exclusively decide the personal data to be collected. Employers do not collect the personal data directly from their employees first and provide this to us. Rather, individual employees come directly to us with this data. Profile recipients are then able to access their Profiles independently, on our online service. It is then for those recipients to decide what they choose to do with their Profiles.

Additionally, we:

- Decide the applicable retention periods for the personal data within Profiles. We do not act on the instructions of employers in relation to this data.
- Determine the content of our privacy policy that is issued to Profile recipients. We would not take instructions on the content of our privacy policy from employers;
- We notify individuals about their rights under data protection law and act on their instructions regarding this data as opposed to the employer; and
- We make independent decisions regarding Profile data. For example, we determine where data is stored and the security measures in place for that data. We would not take instructions from employers on these matters.

We acknowledge that employers may, on occasion, pass us details regarding recipients (such as email addresses). Regardless, we remain of the view that we are a controller in this situation. Data sharing does not change the fact that we exercise overall control of the purpose and means of the processing of personal data in these situations. Processors do not have the same obligations under data protection laws as controllers and we do not believe it is appropriate for us to occupy this role given the above information.

4. Do we comply with data protection laws?

We are an international group of companies. We comply with all applicable data protection

laws where we are active. We have established our global legal framework in line with the General Data Protection Regulation (GDPR) (Regulation (EU) 2916/679) ("EU GDPR"), the UK GDPR (as retained in the EU (Withdrawal Act) 2018 and the Data Protection Act 2018 (DPA 2018). The provisions of the UK GDPR are applied in accordance with the worldwide data protection regulations allowing us to ensure data is protected in accordance with applicable laws in each jurisdiction we operate in.

Where possible, we rely on adequacy for data transfers globally. This means that the data subject will not, during transfer or on receipt by the transferee of the personal data, be subject to a standard of protection lower than that the standard they are provided under UK (or the applicable jurisdiction) data protection laws. We are currently guided by the European Commission adequacy decisions which have been adopted by the UK following withdrawal from the EU.

For any transfer of personal data outside of the UK/EEA, we implement the EU Standard Contractual Clauses ("EU SCCs") as put in place by the European Commission. For personal data transfers relating to UK data subjects, the UK Addendum (as prepared by the ICO) is attached to the EU SCCs. We require that any organisation we engage in a data transfer has appropriate technical and security measures in place to ensure data is adequately protected. In line with the GDPR rules, as the data controller who transfers the personal data, we are the data exporter.

We follow developments of UK data protection law closely and will make any necessary amendments to our data protection processes following legislative changes. We will communicate any material changes we make with our clients and data subjects within 30 days.

5. Where do we store personal data?

All personal data collected through our online evaluator questionnaire is stored online in our web application. Insights Online data is hosted by Amazon Web Services (AWS) in an ISO 27001 certified data centre in the UK. New Customer Platform data is hosted by Amazon Web Services (AWS) in an ISO 27001 certified data centre in the EU. Personal data collected through other means, including contact details of our customers, personal data regarding accreditation or workshops conducted by us are stored in IT services managed by us.

6. What technical-organizational measures have we implemented?

We employ a range of technical and security measures to ensure compliance with data protection laws and the safeguarding of personal data.

We rely on certified data centres for secure data storage and processing and require encryption, where possible. For more information about AWS security measures, visit ISO/IEC 27001:2022 Compliance - Amazon Web Services (AWS).

Our information security management system is currently based on ISO 27001 and follows

recommendations from NIST Cybersecurity Framework. We achieved ISO 27001:2022 accreditation in November 2023. This accreditation requires a set of standards for systems to ensure that all legislative and regulatory requirements are adhered to. This certification illustrates the commitment that we have to the security of data and systems to support data handling.

We also ensure that:

- A disaster recovery plan is in operation with recovery time objectives, with scheduled annual tests
- Penetration testing is regularly conducted on all systems to ensure compliance
- Any third party providers are vetted for compliance with CREST certification
- Data monitoring is continually in operation during storage to ensure data integrity
- Data is securely disposed of and security logs retained for a period of 180 days (effectively around 6 months)

7. Who do we transfer personal data to?

We will share personal data as specified in in our privacy policy. For example, we share Profiles with Profile recipients and the Accredited Practitioner.

We share 'Team Wheels' or aggregated reports (but never Profiles) with the organisation that ordered the workshop or individual debriefing for the purpose of team effectiveness training.

We do not use data for purposes other than those described in privacy policy and we do not sell information to third parties.

We do not typically engage any processors but may occasionally utilise third party printers for the printing of Profiles, where necessary. Any third parties we engage as processors are required to comply with applicable data protection laws. They must also satisfy us that they have implemented adequate safeguards to ensure any personal information is protected.

8. How can Profile recipients exercise their rights?

Profile recipients should contact us at dpo@insights.com to exercise their rights under applicable data protection laws.

9. Who is responsible for information security at Insights?

Our Head of Security is responsible for the security of all data here and can be contacted at: security@insights.com

10. Has Insights appointed a data protection officer?

Yes. Our DPO is based at our headquarters in the UK and can be contacted at: dpo@insights.com.

As of January 2025