Investors in People Data Security / Protection FAQs

Question	Response
Is IIPCIC registered with the Information Commissioners Office?	Yes, registration number: ZA286529
Does IIPCIC have a Data Protection Policy?	Yes – please see the Data Protection section on our website: https://www.investorsinpeople.com/data-protection/
Are IIP classed as a Data Processor?	No, IIP has a controller to controller relationship with both clients and Practitioners who deliver the IIP service. A data controller is an organisation that determines what data is needed, what can be done with it, and how to handle that data – we therefore need to process the data according to our processes, in particular the data used within our online assessment system.
What physical security controls are in place to protect personal data?	Building entry controls: We work in a government secured building where only people with valid photo identification can enter and all entries to our building are manned by security personnel. Doors on each floor are electronically locked. ID and access control cards required to enter the floor.
What maintenance programme/s do you have in place to ensure that your computer equipment and software is kept running smoothly and to fix any security vulnerabilities?	All servers and networking equipment is monitored and proactively managed by our IT Manged Service Provider, this includes 24/7 monitoring and resolution of issues as well as proactive maintenance, updates and security fixes, vulnerability scanning is performed regularly, and actions taken to close any identified issues.
Is IIP certified in an industry accepted control standard?	We are working towards Cyber Essentials Plus.
Are your Information Security policies reviewed and updated periodically?	Yes, annually. Our Managed Service Provider also provides regular updates, monthly emails, staff training sessions as well as IT Steering Group sessions to ensure we are kept up-to-date with current and emerging IT security issues.
Do IIP employees receive data protection training?	Yes, at recruitment and this is refreshed periodically.
Are IIP employees asked to sign a data protection policy as part of their terms and conditions of employment?	Yes
Are contractors and part-time/temporary employees	Yes

bound by your information security policy, and confidentiality and/or non-disclosure agreements?	
Do you use Antivirus software on all employee desktops, laptops, and servers?	ESET Endpoint protection is installed on all user devices, updates are monitored.
What firewalls/network security are in place?	A fully managed 100Mb dedicated wireless solution with a Cisco 891 router/firewall is in-place.
Do you perform periodic vulnerability scanning against your systems?	Vulnerability scanning is performed every 6 months by Mintivo (IT Managed Service Provider), actions are taken on any issues found, currently there are 0 outstanding risks present.
Can I request to see what personal data you hold about me?	Yes, as set out in Article 15 of the GDPR, data subjects have the right to obtain from IIPCIC, where we are the data controller, confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to the personal data and the following information. Please see the Subject Access Request section on our website: https://www.investorsinpeople.com/data-protection/
Do you have a data breach process?	Yes – please see the Data Breach Process section on our website: https://www.investorsinpeople.com/data-protection/
Who do I contact with questions about data protection?	info@investorsinpeople.com
Who is your Data Protection Officer?	IIP do not have a Data Protection Officer, Richard Bell info@investorsinpeople.com is responsible for overseeing our Data Protection strategy.

IIP Assessment Survey

Question	Response
What information is collected from organisations?	Organisations undertaking the IIP survey send us employee names and email addresses so that we can create unique submission links and email their survey links out directly

What information is collected from participants on the IIP survey?	Participants may be asked to submit information about themselves when completing the survey. This information may include, for example: their views about their employer, age, managerial level, gender, or length of service. Most such data is collected in the form of responses to the Likert scale (strongly agree, agree, neither agree nor disagree, disagree, strongly disagree), though other data is collected via multiple choice 'tick boxes' and free-text fields. Multiple choice questions include a 'prefer not to say' response.
Can my organisation see my answers to the IIP survey?	No, all data is aggregated and anonymised removing any Personal Identifiable Information (PII) before being shared with your organisation and any third parties such as Practitioners, delivery partners and other administrators. For the protection of small groups where data trends could be interpreted and linked back to individual submissions, aggregated group data is not shown until there are at least seven responses in the group in question.
Where is survey data, including personal data, stored and how is it kept secure?	Survey data, including personal data, is stored securely within Amazon Web Services. The entire data application (instances, databases, snapshots, backups) is stored within the EU-West-1 (Dublin) data centres, and so adheres to EU controls limiting storage within the EEA. Direct access to the data (databases, snapshots) is limited to senior database architects using asymmetric key-based authentication, and further secured with strict ACLs requiring access through secure Cisco VPNs. Our architects are all security cleared with an Enhanced DBS, and have all been involved in the IIP projects for more than three years. Access to servers is restricted with ACLs, Security Groups, and iptables for instance-specific controls. Backups are run nightly and replicated to a S3 bucket in an AWS region (eu-west-1 - Dublin). For further information on AWS security, including physical access control, auto-replication (redundancy), hypervisor security, and power/infrastructure redundancy, please see: https://aws.amazon.com/compliance/. Application passwords are managed using Drupal - passwords are salted and re-hashed multiple times. Plain-text passwords are never stored in the database. Brute-force attacks are mitigated by auto-blocking login attempts after five failed attempts. Once logged-in, the system supports full RBAC, with minimum-granted permissions (user permissions are granted only when needed for a user account, rather than granting system-wide access). All communications with the site are via HTTPS, using HSTS and modern cipher suites (TLS1.0+). Ciphers are reviewed regularly to ensure security compliance. The system scores the top mark (A+) with independent access check from SSL Labs (https://www.ssllabs.com/ssltest/analyze.html?d=www.investorsinpeople.com).
How long is data stored for and when is it deleted? What happens when data is deleted/archived?	Shortly after an online survey closes it has to be archived in order to reveal full results data. Once a survey has been archived, personal names and email addresses are anonymised using asterisks and the email body is wiped. This process occurs weekly and is irreversible.

How/when is personal data moved and what measures are in place to ensure its security during transfer?	Data is transferred between IIP web systems, including CRM, website and survey platform, using custom built APIs (e.g. between Roden & Gene); these APIs are not publicly documented which provides a layer of security through associated obscurity. Data is encrypted during transit (both between servers and between web server and client) using industry-leading HTTPS configurations. All API transactions are completed at server level; not through Javascript or other frontend code, so cannot be "sniffed" by code inspection from publicly visible code.
Can an organisation undertake the IIP survey without providing any of their staff personal data?	Yes. Surveys operating using only 'open access' links do not require name/email address data.
Who has access to Survey personal data?	In terms of account management, the following users have access to an organisation's data: • Development Partner Organisation • IIP Head Office admins (assigned and given access by the development partner or other IIP Head Office admins) • Administrators from the specific Delivery Partner that works with the client (assigned and given access by the Development Partner or other IIP Head Office admins • The client's Practitioner (assigned, given access, and /or removed by the Delivery Partner admin) * * Please note: Practitioner access to 'Manage Emails' page may be removed.
How are permissions set to ensure only those who truly require it have access to data sets?	Permissions are managed in house – as part of the new starter process, staff are added to the platform and permission levels set in line with their role.
Do we share personal data with other organisations?	All data is for the sole purpose of providing the services to the organisation that is undertaking the survey or other associated project. However, for the purposes of providing the Survey product only, it is sometimes necessary for us to share/make accessible personal data and/or email data with third party organisations.
Which third parties do we share data with? What data do they have access to and how do they keep it secure?	We use an external Development Partner Organisation to build and maintain our online platforms and sometimes to resolve issues with the site. As such, they require access to a minimum amount of personal data. As part of their contract with us, they are subject to an NDA agreement, which binds them by confidentiality and data privacy rules.