Data Protection Policy

Last updated: 29 May 2018

Contents

1. Policy statement

IIPCIC takes its responsibilities with regard to the management of personal data and meeting the requirements of the General Data Protection Regulation (GDPR) very seriously. This document provides the framework through which we achieve those responsibilities and meet the requirements.

Further information about the types of personal data we collect, how we collect it and how we use and process it can be seen on the IIPCIC Privacy Notice.

IIPCIC is registered with the Information Commissioner's Office, registration reference: ZA286529

1.1. Data Protection Principles

In accordance with the seven principles of data protection as set out in the GDPR, we will always ensure that personal data shall be:

a) Processed fairly, lawfully and in a transparent manner.
b) Collected for specified, explicit and legitimate purposes only.
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d) Accurate and up to date.
e) Kept in a form which permits identification of data subjects for no longer than is necessary.
f) Processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

1.2. Notifying Data Subjects

Whenever we collect personal data directly from data subjects, we will inform them about:

- The purpose or purposes for which we intend to process that personal data.
- The types of third parties, if any, with which we will share or to which we will disclose that personal data.
- How they have the right to access their personal data.
- How they have the right to have their personal data rectified if it is inaccurate or incomplete.
- How they have the right to request the deletion or removal of their personal data where there is no compelling reason for its continued processing.

1.3. Data Security

We have put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

As at May 2018 we are currently working towards achieving the Cyber Essentials Plus certification.

1.3.1. Security procedures include:

- Building entry controls. We work in a government secured building where only people with valid photo identification can enter and all entry and exit points to the building are manned by security personnel.
- Doors on each floor are electronically locked. Electronic access control cards are required to enter the floor. Staff only have access to the floor/Department in which they work.

- Becrypt security is on all staff laptops to prevent unauthorised log-in.
- All IIPCIC staff must adhere to our internal IIPCIC staff data protection guidance policy – see s1.4 for a summary of staff responsibilities.

1.3.2. File storage: System security protocols

All personal data stored on the following are on servers located within the European Economic Area (EEA):

File storage: IIPCIC uses cloud based Box and Microsoft Office 365:

- For Box security protocols please see the following link: https://cloud.app.box.com/v/RedefiningContentSecurity
- For Microsoft Office 365 see: https://support.office.com/en-us/article/overview-of-security-and-compliance-in-office-365-dcb83b2c-ac66-4ced-925d-50eb9698a0b2

1.3.3. IIP Online Survey

Survey data, including personal data, is stored securely within Amazon Web Services (AWS). 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.

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.

1.3.4. IIP CRM

The IIP CRM is a web based application and follows the AWS security and storage controls as detailed in 1.3.3 above. The following data is held on the IIP CRM:

- Organisation name, address, telephone number(s) and generic email address.
- Client contacts names, email address(es), job title and phone number(s) of those who are working with IIP on an assessment or who have requested further information about IIP products and services.
- Dates to manage the organisation accreditation period including accreditation start date, end date and review dates.
- Other demographic information about IIP accredited organisations including sector (SIC code), size (number of employees) and industry sector (public, private, voluntary).

1.4. IIPCIC Staff responsibilities

All IIPCIC Staff members, whether permanent or temporary, receive data protection training according to their roles and level of responsibilities. We have a staff guidance policy for data protection which includes requirements that:

- All personal data is processed fairly and lawfully in accordance with individuals' rights.
- All personal data is stored securely only in IIPCIC approved locations.
- All data is kept accurate and up-to-date.
- Personal data is kept in accordance with the IIPCIC retention schedule.
- Any data protection breaches are swiftly brought to the attention of the Business Services Director and that they support in resolving breaches.
- Where personal data is to be transferred, then the IIP data transfer policy is observed including considering the necessity of the transfer, the most appropriate method of transfer and the steps to take to ensure the security of the data during transfer.

1.5. Retention of data

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to safely and securely destroy or erase all personal data which is no longer required. This will vary dependent on what data has been collected and for what purpose. Please see our Privacy Notice for the various ways we process data.

1.6. Subject access to personal data

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:

- the purposes of the processing.
- the categories of personal data concerned.
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations.
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- the right to lodge a complaint with a supervisory authority.
- where the personal data are not collected from the data subject, any available information as to their source.
- the existence of automated decision-making, including profiling.

Any individual wishing to exercise this right should follow the Subject Access Request process on the IIP website or email info@investorsinpeople.com with the title 'Subject Access Request'.

The IIPCIC aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within the one month limit set out in the GDPR.

1.7. Right to erasure or Right to be forgotten

The GDPR, Article 17, introduces a right for individuals to have personal data erased. This right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure

verbally or in writing to IIPCIC. IIPCIC will respond within one month to each request but please note that the right is not absolute and only applies in certain circumstances.

1.8. Third parties

IIPCIC may employ the services of a third party to help us in certain areas. In some cases that third party may receive your personal information either directly from IIPCIC or direct from the client they are working with. Where IIPCIC controls the use of this personal information, it will ensure that all third parties do so as data processors, and that they have appropriate technical and organisational measures in place to protect the data and process it in accordance with this data protection policy. Where the third party is contracted to work with you e.g. an IIP Practitioner or Delivery Partner they will sometimes collect personal data directly. In this case they are a joint data controller and you may wish to inform yourself of their privacy notice. See section 3 of the IIPCIC Privacy Notice for more information.

For clients/individuals within the EEA we do not share your personal data outside of the EEA. Where clients/individuals are outside the EEA we ensure that the information has equivalent protection as if it were being processed within the EEA by entering into a Data Sharing Agreement which contains model EU clauses.

1.9. Data Breach

A data breach may mean that someone other than the data controller gets unauthorised access to personal data but a data breach can also occur if there is unauthorised access within an organisation, or if a data controller's own employee accidentally alters or deletes personal data.

Following a report or a data breach or suspected data breach the IIPCIC will confirm whether a breach has occurred and assess the risks associated with it. This includes:

- the nature of the breach.
- an indication of the seriousness of the breach.
- any action IIPCIC must take immediately (i) to contain the breach and (ii) to become compliant with the GDPR and/or (iii) to prevent a similar situation from arising in the future.

All notifiable breaches will be reported to the ICO within 72 hours of IIPCIC becoming aware of it. We will notify organisations whose personal data is affected by the breach within 24 hours of becoming aware of it.

1.10. More information

If you have any queries regarding IIPCIC's data protection policies please contact: info@investorsinpeople.com