Ixion

Data Protection Guidance Notes

Data Protection Guidance Notes

These Guidance notes underpin the Data Protection Policy. The guidance notes are group wide Shaw Trust guidance for all employees in the Shaw Trust Group.

The objective of these Guidance Notes is to give guidance and direction to employees and managers who process personal information about an individual. This type of information is called Personal Data under the Data Protection Act 1998 (DPA). The Data Protection legislation affects all of Ixion's business as will, with effect from May 2018, the requirements contained within the General Data Protection Regulation (GDPR).

They also give guidance on the release of personal information to the Police.

References in these notes to a Delivery Programme apply to all programmes where Ixion is contracted to a commissioning body to deliver services to customers.

1. Background

At present, the processing of personal data is controlled by the DPA. On 25th May 2018, the General Data Protection Regulation (GDPR) will come into effect and will be directly applicable in all EU Member States, without the need for implementing national legislation. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR. The principles of the GDPR are similar to those of the DPA, with added detail at certain points and a new accountability requirement.

The most significant addition is the accountability principle. The GDPR will require Ixion to show how it complies with the principles: for example by documenting the decisions taken about a processing activity.

For the purpose of these Notes and at this time, it is assumed that the provisions of the GDPR will be included in a new version of the DPA and that definitions will be broadly similar to existing definitions.

2. Key Definitions

- **Personal data**
  Information about a living individual who can be identified from that data, or with other data in the possession of the data controller or the data processor (e.g. name, address, DOB, NI number, someone's photograph, CCTV image, voicemail message etc.). N.B. personal data includes expressions of opinion about an individual and any indication of the intentions of the data controller in respect of the individual. Ixion processes the personal data of customers (e.g. learner records and plans, assessments, CVs, action plans etc.) and employees, volunteers, interns etc. (e.g. HR records, 1-1 review forms etc.).
- **Sensitive personal data**
  Data about a person's ethnicity, political opinions, religious beliefs or beliefs of a similar nature, TU membership, physical or mental health or condition, sexual life, the commission or alleged commission of offences, any proceedings for an offence and the sentence or disposal of such proceedings. Note: in the GDPR, sensitive personal data is referred to as "special personal data".
- **Data Subject**
  Any living individual, including a child, can be a data subject. Companies cannot be data subjects but employees or directors of companies are data subjects.
- **Processing**
  Collecting, organising, holding, adapting, altering, retrieving, combining, consulting, using, disclosing, erasing any data etc.
  This data may be held electronically or physically, as hard copy.
- **Data Controller**
  An organisation which determines the purpose and manner in which data is to be processed. Except for customer personal data obtained by Ixion as part of a Delivery Programme, or other situations in which Ixion processes personal data on behalf of a third party, the data controller will be Ixion, as it is Ixion

which determines the purpose for which, and the manner in which, personal data is processed. However, in the case of customer personal data which has been obtained during the course of delivering a Delivery Programme (whether the data has been provided by the contracting body or by the customer), the contracting body is the data controller and Ixion is the data processor.

Therefore, all customer data is subject to the contracting bodies' data security requirements.

Ixion is data controller in respect of the personal data of (not exhaustively):

- Full and part time employees
- Interns
- Apprentices (of Ixion)
- Volunteers
- Job Applicants
- Consultants

- **Data Processor**

  An organisation which processes data on behalf of a data controller (under a contractual agreement such as a Delivery Programme).

3. General:

- It is the responsibility of the Head of Service - IT to maintain these Guidance Notes, to review them on an annual basis and to ensure their continuing relevance.
- All employees, as well as volunteers, interns and contractors, of Ixion are responsible for the implementation of these Guidance Notes.
- These Guidance Notes should not discourage Ixion staff from making full use of the filing, computer, ICT, internet and email systems.
- The Compliance Officer for data protection is the Head of Service - IT.

- Failure to comply with these Guidance Notes could result in disciplinary action being taken against the member of staff involved. In certain circumstances, the staff member could be held criminally liable if he/she knowingly or recklessly discloses personal data in contravention of the Data Protection Act. Such action may be treated as gross misconduct which could result in summary dismissal.
- The Head of Service – IT will maintain a risk register, which will be reviewed annually. This Register will record the likelihood and severity of the risk to the rights and freedoms of data subjects.

4. The 8 Data Protection Principles of the DPA:

- Personal data is to be processed fairly and lawfully
- data is only to be used for specified purposes
- data processed should be adequate, relevant and not excessive
- data should be accurate and kept up to date
- data should not be kept for longer than necessary
- data should be processed in accordance with the rights of data subjects
- appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data, and against loss or destruction or damage to personal data
- data should not be transferred to a country outside the EEA.

5. Data Subjects' Rights under GDPR:

- The right of access by an individual (subject) – see 6 below.
- The right to object to processing that is likely to cause damage or distress to him/her or another individual – see 7 below.
- The right to require the data controller to ensure that no decisions are taken by the data controller which significantly affect the individual that are based on processing personal data by automatic means for the purpose of evaluating

matters relating to him/her, e.g. performance at work, his/her reliability or conduct etc.

- The right to apply to court for an order that requires a data controller to rectify, block, erase or destroy inaccurate data – see 8 below.
- The right to prevent processing for direct marketing.
- The right to compensation if the data subject has suffered financial loss or distress.

Note: the GDPR will contain more robust and far-reaching rights.

6. Handling a Subject Access Request (SAR):

A data subject has the right to request access to his/her personal data processed by a data controller, provided the request is in writing and the maximum statutory fee received (currently £10). The data controller has to respond promptly and within 30 calendar days with copies of the data. A SAR received by a data processor should be passed to the data controller to deal with. If any member of staff receives a SAR, refer to the Access to Personal Data by a Data Subject Procedures. Note: under the GDPR, copies of the information must be provided free of charge, subject to certain exceptions.

7. A customer on a Delivery Programme refuses to provide personal data (e.g. mobile phone number, email address etc.) or refuses to give consent Ixion to process their personal data:

An individual can refuse to provide personal data and can withdraw his/her consent to processing or limit the processing Ixion does of his/her personal data if he/she can show it is or would cause him/her or another damage or distress. The individual must be able to show that the processing is or would cause unwarranted and substantial financial loss or physical harm and substantial distress, i.e. a level of upset that goes beyond annoyance or irritation. An individual has no right to object to processing if:

- he/she has already consented to the processing or

- the processing is necessary for a contract that the individual has entered into or
- the individual has asked for something to be done so he/she can enter a contract or
- the processing is necessary because of a legal objection that applies to the data controller (except a contractual obligation) or
- the processing is necessary to protect the individual's 'vital interests' (a life or death situation).

If Ixion can show that the processing the individual has objected to Ixion may be able to refuse to accept the objection and provide an explanation, e.g. if the individual has requested that personal data supplied by him/her is destroyed, Ixion can refuse to destroy such data if it is contractually obliged to hold data for a specified period.

Write to the Shaw Trust Group wide Data Protection Officer at sejal.patel@shaw-trust.org.uk if a request is received to cease processing a customer's personal data which goes beyond withdrawing or refusing consent to Ixion sharing data with a third party employer.

8. A data subject requests Ixion to correct or erase inaccurate data:

If Ixion receives a request to correct data, it will consider the request and respond within 21 days to confirm whether or not the objection is accepted. If Ixion accepts that it is inaccurate, it should correct the record and ensure that any third parties that it has shared the data with are notified of the correction. If Ixion receives a request to correct data that it does not accept is inaccurate, it should write to the individual within 21 days to explain why it does not intend to amend its records and hold the request on file with the data.

9. Where may Personal Data be found and how should it be stored and transferred:

Personal data may be held or stored on computers, videos, compact discs, tapes, email, electronic and paper filing systems, rollerdex cards, electronic organisers or any other general filing system.

An individual's photograph taken for Ixion's business is likely to constitute personal data (and shall be treated as personal data). If you intend to take film or photographs of customers contact the Head of Service - IT, who will request that the customers sign a Publicity Consent form before the film or images are taken.

In addition to the requirements contained in the DPA, Ixion has a contractual obligation to process and store all customer personal data obtained in the course of delivering Delivery Programmes in accordance with strict procedures, which are more fully detailed in the Physical Security Procedures, Data Encryption Procedures, Email and Communications Guidelines, the Exchange of Classified Information Procedures and other relevant documents in our Information Security Management System. All staff members, volunteers and interns must be fully aware of and comply with these requirements.

Disciplinary procedures may be taken against any member of staff who breaches the data protection legislation and these procedures and, in serious cases, such violation may be treated as gross misconduct which could result in summary dismissal.

10. How the Data Protection Principles Affect You:

- The Data Protection Act 1998 and subsequent legislation applies to all personal data which we process and will include records held on computerised systems and manual data held in any filing system where the data can be found by reference to an individual's name, address, employment or other criterion. This means that any information which is organised in a structured way is likely to be subject to these principles.
- Ixion will only process personal data fairly and lawfully. Staff need to explain to customers that Ixion will undertake the processing and sharing of their data in

compliance with GDPR In the past, we have done this by issuing customers with an advisory leaflet at Induction (where the referral is received under a sub-contract) or in the Welcome Pack (where the referral is received under the prime contract). This process will continue, where Ixion is not the sole Data Controller, insofar as compliance with the data protection principles is concerned. If a customer objects to Ixion processing his/her personal data, please inform the Head of Service - IT, who will advise on how to proceed.

- Where Ixion is the sole / joint Data Controller or a Data Processor, insofar as compliance with the data protection principles is concerned, the following classes of data subject will be issued with Privacy Notices:

    - Customers including Learners
    - Employees, Job applicants;
    - Donors, Fund-raising participants;
    - Individuals who upload personal data to websites;
    - Individual consultants and contractors;
    - Referees and Emergency Contacts for Volunteers;
    - Volunteers

  Ixion must ensure that all personal data which it processes is accurate and kept up-to-date.

- Employees should ensure that, when requesting personal details (for example, from a customer, another employee or contact at a donor company), they only request personal details which are absolutely necessary. We should not request or hold excessive personal information.
- Ixion should only process sensitive personal data where this is necessary.
- Employees must be vigilant to ensure that personal data and, in particular, sensitive personal data which Ixion holds and processes is kept secure so that the risks of damage, destruction, loss, theft or deletion are minimised.
- In no circumstance should an employee sell, dispose, use or process personal data or sensitive personal data for purposes not connected with the business of Ixion. If an employee knowingly or recklessly discloses personal data in

contravention of Ixion's policies and procedures, he/she may face disciplinary sanctions as well as criminal penalties.

11. Police Enquiries

a) Regarding non-criminal activity:

In the event of a request from the Police for the release of a customer's personal data because they have a concern over that customer's safety, the following notes summarize the position of the Information Commissioner's Office:

- Schedule 2.4 of the DPA states that processing (sharing data) is permitted where

  *The processing is necessary in order to protect the **vital interests** of the data subject.*

  Potential suicide falls within this category, but you must be satisfied that it is a matter of life and death

- Schedule 3.3. of the DPA states that processing (sharing data) is permitted where

  *(a) in order to protect the **vital interests of the data subject or another person**, in a case where—*

  (i) consent cannot be given by or on behalf of the data subject, or

  (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

  *(b) in order to protect the **vital interests of another person**, in a case where consent by or on behalf of the data subject has been unreasonably withheld.*

  This indicates that you could disclose to the Police the personal data (e.g. name and address) of next-of-kin.

- To release personal data in a missing persons case is not so clear-cut, since one must make a judgement as to whether the fact that the person is missing indicates that the person's vital interests are at risk, or whether the absence is less sinister. The Police would need to give sound reasons as to why they are concerned.

However, the over-riding principles in all cases are:

1. It is for Ixion to make the judgement as to whether to release information, in the light of the evidence given to us
2. We must ensure that we release any such data to the proper person, and that that person is giving a valid and true reason for the request (e.g. that the Police are not asking for the information in order to follow up other enquiries)
3. In order to satisfy ourselves re 2 above, we should get the request in writing, with a stated reason for the request and why the Police are concerned
4. We must be able to show that we have followed process (strong audit trail), with documentation every step of the way, explaining why we are taking each action
5. Before releasing information, details regarding clauses 11.2 to 11.4 must be submitted to the Data Protection Officer, who will make the ultimate decision over whether to release or not
6. If the individual later complains to the ICO, and we have the above in place, showing that we have dealt with each case in good faith and on the basis of the best information we can get, the ICO is unlikely to conclude that there has been a breach of the Act.

b) Regarding criminal activity:

- In the event of a request from the Police for the release of a customer's personal data because it is needed to prevent or detect a crime, or catch and prosecute a suspect, the following guidance from the ICO explains what Ixion needs to consider when it is asked to release personal information:
    - There is an exemption in the DPA that allows Ixion to give out personal information for these purposes, but there are limits on what we can release.
    - The exemption does not cover the disclosure of all personal information, in all circumstances. It only allows us to release personal information for the stated purposes and only if not releasing it would be likely to prejudice (that

is, significantly harm) any attempt by police to prevent crime or catch a suspect.

- For every request for personal information you receive (and about each separate individual), you need to ask yourself the following questions:
  - Am I sure the person is who they say they are? (For this reason particular care should be taken if the request is made over the telephone);
  - Is the person asking for this information doing so to prevent or detect a crime or catch or prosecute an offender?
  - If I do not release the personal information, will this significantly harm any attempt by the police to prevent crime or catch a suspect? (The risk must be that the investigation may very well be impeded.)
  - If I do decide to release personal information to the police, what is the minimum I should release for them to be able to do their job?
  - What else (if anything) do I need to know to be sure that the exemption applies?
- The ICO understands that most people will want to help the police to prevent crime or catch a suspect, but it is up to Ixion to decide to release personal information under this exemption. Even if Ixion decides that the exemption applies, it still does not have to release the personal information.
- If here are genuine concerns about releasing the personal information (for example, because Ixion considers it has other legal obligations such as the information being confidential), then the police can be asked to come back with a court order requiring the release of the personal information. If the court decides we should release the information, we will not break the Act by obeying the order.
- As with non-criminal enquiries:
  - We must ensure that we release any such data to the proper person, and that that person is giving a valid and true reason for the request (e.g. that the Police are not asking for the information in order to follow up other enquiries)

    - We must get the request in writing, with a stated reason for the request and why the Police require the information
    - We must be able to show that we have followed process (strong audit trail), with documentation every step of the way, explaining why we are taking each action
- Before releasing information, the Head of Service -IT must be supplied with all the information, to enable him/her to make the ultimate decision over whether to release or not.

12. Ixion's Management of Data Protection

- Ixion may carry out checks to ensure that everyone is complying with these Guidance Notes. These checks may include, without limitation, occasional audits to check that personal data is being processed fairly and lawfully, spot checks and random searches through records.
- If an employee, volunteer or intern has any questions or is unsure about any of his/her obligations under the Data Protection Act, please contact the Head of Service – IT.

14. Data Deletion and Correction

- Data protection legislation allows for data subjects (in certain circumstances) to request the deletion and/or correction of all or part of the personal data that is held by Ixion.
- Such requests will be received by the Data Protection Officer, who will consider whether they are fair and proper and, if so:
    1. Raise a support IT ticket for the change and/or make the change in the live database
    2. Record the change on the Data Deletion and Correction Record, so that an identical change will be made to backed-up copies of the data, if and when they are restored from back-up to live instance. See Data Deletion and Correction Record form embedded here

Data Deletion and
Correction Record (D

3. Notify the data subject that his/her data has been deleted / corrected from all live instances, but is retained on back-ups, which are “beyond use”, and that, if the data is ever restored, similar deletion / correction will be applied to the restored version.

It must be noted that, in order to comply with legislation, backed-up data need not be deleted / corrected, if it is “beyond use”. To classify as “beyond use” the Information Commissioner’s Office has provided the guidance embedded below.

This guidance must be followed.

ICO Guidance re
Deleting Personal Dat

Additionally, such backed-up data will not be relevant to a Subject Access Request, provided always that it remains beyond use and cannot be interrogated.