Ixion Group Policy & Procedure

Data Subject Request

Data Subject Requests are requests by an individual (a “data subject”) to exercise their rights under “Data Protection Legislation”. They include Subject Access Requests (SARs), which are requests to be told what information a Data Controller holds in respect of the data subject. A SAR and other requests must be in writing (email, electronic or hard copy) – verbal requests do not constitute valid SARs (see clause 4.2 below).

“Data Protection Legislation” comprises the Data Protection Act 1998 (DPA), the General Data Protection Regulation (GDPR) and any subsequent legislation enacted in the UK.
In May 2018, the GDPR will come into effect. It will give data subjects the following rights, some of which are additional to rights under the DPA:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

The objective of this Policy and Procedure is to give guidance and direction on the rights of an individual (customers and others, such as staff, volunteers etc.) and on the obligations of Ixion when dealing with any such requests with which it is obliged to comply.

Important notes:

- These Procedures refer throughout to the processes to be followed when a SAR has been received. The same processes **must** be followed if a data subject has exercised any of the other rights contained within Data Protection Legislation. These rights are listed above. This objective will be achieved through following these Procedures.
- Backed-up data will not be relevant to a Subject Access Request, provided always that it remains “beyond use” and cannot be interrogated. 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

1. Summary:

- A SAR is created by section 7 of the DPA and is repeated in the GDPR. It is most often used by individuals who want to see a copy of their records or any other information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request and pays a fee (if relevant) is entitled to be:

    1. told whether any personal data is being processed;
    2. given a description of the personal data, the reasons it is being processed, and whether it has been given to any other organisations or people;
    3. given a copy of the information comprising the data; and
    4. given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret).

- A SAR must be dealt with promptly and, in any event, within one month of receiving it. However, some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR.
- These Procedures do not cover the requirements for children or for those who lack the mental capacity to manage their own affairs. However, a person must be assumed to have capacity to make the request unless it is formally established that he/she lacks capacity (ref: Mental Capacity Act 2005).
- Further and more detailed information may be found on the Information Commissioner's website at: Access to personal data
- Failure to comply with these Procedures 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 these Procedures. Such action may, in extreme cases, be treated as gross misconduct which could result in summary dismissal.

- The Compliance Officer for data protection is the Head of Service - IT and administration of these Procedures is handled currently by the Data Protection Officer.

  Other Data Subject Requests, which must be handled in the same way as SARs are:

  - requests to have personal data rectified if it is inaccurate or incomplete
  - requests for the deletion or removal of personal data where we are not otherwise entitled to retain and process such data and there is no compelling reason for its continued processing
  - requests to restrict or suppress the processing of personal data, in certain circumstances
  - requests to exercise the right to withdraw consent at any time, where relevant.

2. Procedures for customer data subject requests (inc. SARs)

All employees must remember to ensure they upload any hard copy notes/documentation to the appropriate system so we can ensure we have access to all information held on a customer. Failure to do so may result in an inability to locate the information, leading to a potential breach of Data Protection Legislation.

In the event that an employee receives a request from a customer or third party for details or copies of data that Ixion holds on a customer or other customer data subject request, the following process must be applied:

2.1 The Head of Service - IT must be notified immediately, using Ixion's internal Data Subject Request Form template and attaching a copy of the customer's written request. The Head of Service - IT may be contacted here – sar@ixionholdings.com

2.2 The Head of Service – IT will:

- Validate the identity of the requestor and then send an acknowledgement to the individual or third party within two working days of receiving the notification; if requested, provide the customer or third party with the Data Subject Request Form, which the customer will need to complete and return to the Head of Service - IT; seek confirmation of the precise scope of the customer's written request;
- SARs only:

- Notify the relevant Data Controller by sending them a copy of the customer's written request and acknowledgement in a timely manner and, in any event, in accordance with contractual requirements.

- **Where a third party (e.g. a commissioning body such as DWP or ESFA) is the Data Controller and Ixion is Prime Provider:**
  - Send the customer's written request to the third party's applicable Data Protection Officer (DPO) who will process the request and liaise with the individual or third party. The DPO will also liaise with Ixion to obtain copies of records and/or information;
  - Collate and copy all data Ixion holds on the customer. This may be paper-based or held electronically on Ixion systems or any other computer device. In particular, the Head of Service - IT must consult all archived hard-copy and electronic records, to ascertain the occasions on which the Data Subject is / was a customer of Ixion and whether these occasions fall within the scope of the customer's written request;
  - Send hard copies of data to the third party's Data Protection Officer either by courier or by Royal Mail's Special Delivery (Track & Trace) service or to an individual and in a manner as shall be notified to Ixion by each third party. Electronic copies will be encrypted in accordance with the Exchange of Classified Information Procedures.

- **Where a third party (e.g. a commissioning body such as DWP or ESFA) is the Data Controller and Ixion is sub-contracted to another Prime Provider:**
  - Send the customer's written request to the Prime who will process the request and liaise with the Data Controller – no further action is required by Ixion, unless otherwise notified by the Prime.

- **Where Ixion is the Data Controller:**
  - Process the request and liaise with the individual or third party to send copies of records and/or information.
  - Advise the customer / third party that Ixion will supply copies of the information free of charge, but that a 'reasonable fee' may be charged, when a request is manifestly unfounded or excessive, particularly if it is

repetitive or to comply with requests for further copies of the same information.

- Retain securely a copy of all data supplied for Ixion's records;
- Provide the Ixion Board of Directors with quarterly reports summarising activity and progress on Data Subject Requests and will notify the Executive Board Director should difficulties arise.

Important: The Head of Service - IT will not release copies of any customer personal data without the written authorisation of the relevant Data Controller.

3. Procedures for requests from others

3.1 Managers or staff members who receive a written request from individuals who are not customers (e.g. staff members, volunteers etc.) must notify the Head of Service - IT immediately, using Ixion's internal Data Subject Request Form, and attaching a copy of the individual's written request.

3.2 The Head of Service - IT will liaise with the Head of the relevant department, to ensure that the request is dealt with by that Head of Department in accordance with Data Protection Legislation. In the event of any uncertainty, the Head of Service - IT will consult with the Data Protection Officer and/or seek professional legal guidance.

4. Further detail

4.1 What is an individual entitled to?

Under the right of subject access, individuals are entitled only to their own personal data, and not to information relating to other people (unless they are acting on behalf of that person). Neither are they entitled to information simply because they may be interested in it. Therefore, it is important to establish whether the information requested falls within the definition of personal data. In most cases, it will be obvious whether the information being requested is personal data, but the website above gives separate guidance to help decide in cases where it is unclear.

Subject access provides a right to see the information contained in personal data, rather than a right to see the documents that include that information.

N.B.

1. If individuals ask for copies of their "file", all data held in hard copy or as electronic data on their files must be disclosed;

2. If they ask for all information that Ixion holds, we must disclose all records pertaining to the individual, including emails, handwritten notes, letters etc. following the procedure shown in Sections 2 and 3.
3. See below at 4.10 for restriction and exemptions where data can be withheld.

4.2 What is a valid SAR?

For a SAR or other request to be valid, it must be made in writing. The following points should also be noted when considering validity:

- A request sent by email or fax is as valid as one sent in hard copy.
- There is no need to respond to a request made verbally but, depending on the circumstances, it might be reasonable to do so (as long as one is satisfied about the person's identity), and it is good practice to at least explain to the individual how to make a valid request, rather than ignoring them.
- If a disabled person finds it impossible or unreasonably difficult to make a SAR in writing, a reasonable adjustment may need to be made for them under the Disability Discrimination Act 1995. This could include treating a verbal request for information as though it were a valid SAR. One might also have to respond in a particular format which is accessible to the disabled person, such as Braille, large print, email or audio formats. If an individual thinks Ixion has failed to make a reasonable adjustment, they may make a claim under the Disability Discrimination Act and/or the Equality Act 2010. Information about making a claim is available from the Equality and Human Rights Commission.
    - If a request does not mention Data Protection Legislation specifically or even say that it is a SAR, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data.
- A request is valid even if the individual has not sent it directly to the person who normally deals with such requests – so it is important to ensure all members of staff can recognise a SAR and treat it appropriately.

4.3 Can Ixion require individuals to use a specially designed form when making SARs or other requests?

No. Any request in writing must be considered as a valid request, whatever the format. However, Ixion has produced a Data Subject Request form, and we can invite individuals to use this form, as long as we make it clear that this is not compulsory and that we do not try

to use this as a way of extending the one month time limit for responding. This standard form will make it easier for us to recognise a SAR or other request and will make it easier for the individual to include all the details we might need to locate the information they want.

4.4 Do we need to release data which has been processed after the date of the written request?

The Act specifies that a SAR relates to the data held at the time the request was received. However, in many cases, routine use of the data may result in it being amended or even deleted while Ixion is dealing with the request. Therefore, it would be reasonable for us to supply information we hold when we send out a response, even if this is different to that held when we received the request.

However, it is not acceptable to amend or delete the data if we would not otherwise have done so.

4.5 Does Ixion have to explain the contents of the information it sends to the individual?

The Act requires that the information we provide to the individual is in “intelligible form”. At its most basic, this means that the information we provide should be capable of being understood by the average person. However, the Act does not require Ixion to ensure that the information is provided in a form that is intelligible to the particular individual making the request.

4.6 Can Ixion charge a fee for dealing with a SAR?

No. However, a ‘reasonable fee’ may be charged, when a request is manifestly unfounded or excessive, particularly if it is repetitive.

A reasonable fee may also be charged to comply with requests for further copies of the same information. This does not mean that an organisation can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

4.7 Can Ixion ask for more information before responding to a SAR?

The Act allows for Ixion to confirm two things before it is obliged to respond to a request.

1. We can ask for enough information to judge whether the person making the request is the individual to whom the personal data relates. This is to avoid personal

data about one individual being sent to another, accidentally or as a result of deception.

The key point is that Ixion must be reasonable about what it asks for. It should not request more information if the identity of the person making the request is obvious to Ixion. This is particularly the case, for example, when it has an ongoing relationship with the individual.

It is essential to ask the person making the request to verify their identity before sending them information.

2. Before responding to a SAR Ixion is entitled to ask for information that it would reasonably need to find the personal data covered by the request. Ixion need not comply with the SAR until it has received this information. In some cases, personal data may be difficult to retrieve and collate. However, it is not acceptable for Ixion to delay responding to a SAR unless it reasonably requires more information to help it find the data in question.

Ixion should not ignore a request simply because it needs more information from the person who made it. Ixion should not delay in asking for this but should ensure the individual knows it needs more information and should tell them what details it needs.

4.8 SARs made on behalf of others

The Act does not prevent an individual making a SAR via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If we think an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, we may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

4.9 What should we do if the data includes information about other people?

Responding to a SAR may involve providing information that relates both to the individual making the request and to another individual. The Act says we do not have to comply with

the request if to do so would mean disclosing information about another individual who can be identified from that information, except where:

- the other individual has consented to the disclosure; or
- it is reasonable in all the circumstances to comply with the request without that individual's consent.

So, although we may sometimes be able to disclose information relating to a third party, we need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. If the other person consents to us disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, we must decide whether to disclose the information anyway. Where practicable, the other person's personal information should be redacted so as to avoid any danger of improper sharing of that information.

For the avoidance of doubt, we cannot refuse to provide subject access to personal data about an individual simply because we obtained that data from a third party. The rules about third party data apply only to personal data which includes information about the individual who is the subject of the request and information about someone else.

4.10 Can any data be withheld?

There are some restrictions and exemptions to the subject access requests, which may mean certain data can be withheld. In particular, it may be possible to withhold a data subject's personal data in the following circumstances:

- where disclosure would be likely to prejudice the following crime and taxation purposes:
    - the prevention or detection of crime;
    - the capture of prosecution of offenders; and
    - the assessment of collection of tax or duty.
- where the data consists of information for which legal professional privilege (or its equivalent in Scotland) could be claimed;

- where the data comprises a confidential reference that Ixion has given (or is to give) in connection with education, training or employment, appointing office holders, or providing services;
- where the data is processed for management forecasting or management planning and disclosure would be likely to prejudice the business or other activity of Ixion;
- where the data consists of a record of Ixion's intentions in negotiations with an individual, and disclosure would be likely to prejudice the negotiations.

Any decision to apply an exemption or restriction should be taken at an appropriately senior level and the reasons for the decision should be documented. In the event of any uncertainty, the Head of Service - IT will consult with the Data Protection Officer and/or seek professional legal guidance.

4.11 What if sending out copies of information will be expensive or time consuming?

In some cases, dealing with a SAR will be an onerous task. This might be because of the nature of the request, because of the amount of personal data involved, or because of the way in which certain information is held. We are not obliged to supply a copy of the information in permanent form (hard copy) if it would involve disproportionate effort to do so. Ixion must decide whether supplying a copy of the information would involve disproportionate effort. Even if we do not have to supply a copy of the information in permanent form, the individual still has the other basic rights described above.
The Act does not define "disproportionate effort" but it is clear that there is some (albeit limited) scope for assessing whether complying with a request would result in so much work or expense as to outweigh the individual's right of access to their personal data. However, it should be noted that this qualification to the right of subject access only applies in respect of "supplying" a copy of the relevant information in permanent form. Therefore, we cannot refuse to deal with a SAR just because we think that locating the information in the first place would involve disproportionate effort.

The Information Commissioner's Office (ICO) stresses that we should rely on this provision only in the most exceptional of cases. The right of subject access is central to data protection law and the ICO rarely hears of instances where an organisation could legitimately use disproportionate effort as a reason for not allowing an individual to access

their personal data. Even if we can show that supplying a copy of information in permanent form would involve disproportionate effort, we should still try to comply with the request in some other way.

4.12 What about repeated or unreasonable requests?

Data Protection Legislation does not limit the number of SARs an individual can make to any organisation. However, it does allow some discretion when dealing with requests that are made at unreasonable intervals. The Act says that organisations are not obliged to comply with an identical or similar request to one they have already dealt with unless a reasonable interval has elapsed between the first request and any subsequent ones.
The Act gives us some help in deciding whether requests are made at reasonable intervals.

It says that we should consider the following:

- The nature of the data – this could include considering whether it is particularly sensitive.
- The purposes of the processing – this could include whether the processing is likely to cause detriment to the individual.
- How often the data is altered – if information is unlikely to have changed between requests, we may decide that we are not obliged to respond to the same request twice.