Data Subject Access Requests Policy

September 2017

Contents

Introduction

Purpose

The purpose of this policy is to impose policy and procedure in the handling and processing of data subject access requests (SARs).

The Data Protection Act 1998 (DPA) and the new General Data Protection Regulations (GDPR) that come into force in 2018 give every living person (or their authorised representative) the right to request access to information held about them by an organisation irrespective of when it was compiled.

In accordance with their rights under legislation, this policy sets out how to respond to requests for personal information from and about data subjects about whom we hold and process data whether such processing is on behalf of BiP or BiP's customers.

The scope of this policy applies to information that we hold about all current and former customers, users, suppliers, employees and any other party with whom we have or have had a relationship.

A record can be computerised (electronic) and / or manual form (paper files). It may include such documentation as hand written notes, letters to and from other parties, reports, printouts, photographs, video and call recordings.

This policy forms part of the Information Security Management System.

Scope

This policy applies to all BiP departments, employees, contractual third parties and agents of BiP with access to BiP's information systems.

This policy applies to assets owned or leased by BiP or to devices that connect to a BiP network or reside at a BiP site.

Risks

Non-compliance with this policy could have a detrimental impact on the rights of individuals as data subjects and may result in financial loss and an inability to provide necessary services to our customers.

GDPR and data subject's rights

The GDPR states that data subjects have the right of access to personal data which have been collected concerning him or her, and must be able to exercise that right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing.

Under the GDPR, every data subject has the right to know the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.

Where possible, the data controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.

These rights should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the data controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

Data subjects have the right to obtain confirmation as to whether or not personal data concerning him or her are being processed. Where this is the case, they also have the right to access 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
- Where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period
- The right to lodge a complaint with a supervisory authority

- Where personal data are not collected from the data subject, any available information as to their source
- Where automated decision-making exists, including profiling, meaningful information about the logic involved as well as the envisaged consequences of such processing for the data subject.

The data controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the data controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The right to obtain a copy of the personal data shall not adversely affect the rights and freedoms of others.

Data subjects also have the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.

Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 of the GDPR relating to the transfer.

What is a subject access request?

The DPA and GDPR gives individuals (data subjects) a number of rights including the right to access personal data that an organisation holds about them. This right of access extends to all information held on an individual and includes but is not limited to personnel files, data-base records, interview notes, emails, and financial transactions referring to the individual. If an individual makes a request to view their information, it is known as a "Subject Access Request".

Submission of requests

BiP cannot require anyone to complete a subject access request form, but we can encourage people to use the form as it provides helpful prompts to focus the request and help us identify where the relevant information is likely to be held.

If someone asks for assistance in completing a request form, it can be helpful if a member of staff completes the form and asks the applicant to affirm that the details are correct and to sign it.

It should be noted that people do not have to state that they are making a data subject access request, or cite the Data Protection Act or the GDPR, for their requests to be valid. A request by an individual for their own personal data may be simple or complex. The management of all such requests must be governed by a common set of rules, which are set out in this policy.

Proof of identification

The GDPR explicitly enables controllers to require data subjects to provide proof of identity before giving effect to their rights. This helps to limit the risk that third parties gain unlawful access to personal data. However, the GDPR does not oblige controllers to seek out information to identify data subjects.

If the person making the request for their own information (the data subject) is not known to the person receiving the request, it may be appropriate to obtain proof of identity from the data subject. This would normally be where there are reasonable doubts concerning the identity of the person making the request.

In such circumstances, efforts should be made to request the provision of additional information necessary to confirm the identity of the data subject. This will depend on the circumstances associated with the request, but examples of additional information might include:

- If a request is made verbally, then confirming certain unique attributes may be required
- If a request is made in writing, then it may be appropriate to contact the requestor via an alternative method to confirm it is them who genuinely made the request

If in doubt, advice can be obtained from the Data Protection Officer.

Timescales for complying with requests

In accordance with the GDPR, BiP will respond to Subject Access Requests without undue delay and at the latest within one month. Where BiP does not intend or is unable to comply with a request, reasons must be given. If the request is very vaguely worded, it may be legitimate to stop the clock until clarification can be obtained in relation to the information requested.

Informing applicants of their rights

The person managing the request should consider whether the applicant should be informed of their rights within the acknowledgement and response communications. Appendix 1 provides a summary of the rights of individuals in relation to personal data processing. This can be used to provide information for applicants about their legal rights and to support staff in responding consistently and appropriately to requests.

Responding to simple requests

Whilst data subjects are entitled to request ALL the information an organisation holds on them, experience shows that they are usually looking for something specific. Therefore, the majority of requests received by BiP are likely to be from staff asking for copies of a specific document(s) or from customers asking for information relating to their user accounts and subscriptions.

In the case of staff, this information will usually be located from a single source - typically the staff files staff files staff fustafdepartmental or Human Resources - and will not involve the disclosure of information relating to a third party (see Third Party Data below for more detail). In such cases, BiP policy is to be open and transparent and wherever possible to let the individual have a copy of the information with minimum fuss. Such requests should be handled directly by the relevant department or section and there should be no need to involve the Data Protection Officer. When responding to such requests, take care to ensure you do not inadvertently release third party information without consent (see Requests Involving Third Party Data for further detail). No fee should be charged.

In the case of customers, the information will usually be located in either our Customer Relationship Management system, the service system administration tools, or in the accounting system.

Responding to complex requests

There may be some instances when a request for information is more complex and will need to involve the Data Protection Officer to ensure a co-ordinated response. It is hoped that such requests will be infrequent.

Examples of situations where more complex requests might arise include:

- Request involves locating information from multiple sources
- Request involves the release of contentious information
- Request is one in a series of requests from the same individual
- Request involves the release of third party data for which consent has been refused or cannot be obtained (see Requests Involving Third Party Data information)
- The data subject does not want to ask for the information from the department that holds it

In such cases, the request should be referred to the Data Protection Officer who will ensure that a co-ordinated approach is adopted. The Data Protection Officer will also determine whether or not it is appropriate to charge a fee.

When responding to Subject Access Requests, the Data Protection Officer will liaise with staff in the relevant department as appropriate.

Requests involving third party data

Occasionally, a response to a Subject Access Request may lead to or require disclosure of details relating to some other third party (for example, a manager or colleague, or another customer such as a procurement officer). Such third party information should not be disclosed without first seeking the consent of the third party.

If consent cannot be obtained (e.g. the third party cannot be contacted) or is refused, then the BiP needs to consider whether or not disclosure is reasonable, taking into account:

- Any duty of confidentiality owed to the third party
- The steps taken to seek consent
- Whether the third party is capable of giving consent
- Any express refusal of consent

If you are unable to obtain consent, you should contact the Data Protection Officer who will have to consider/balance the impact on the third party of the disclosure, and the impact on the data subject of the disclosure being withheld. Where third parties have been acting in an official capacity it may be argued that the duty of confidence is lower than is otherwise the case. However, decisions will be made on a case by case basis.

If the Data Protection Officer decides that disclosure cannot be made, only that information which could identify the third party should be withheld (e.g. third party details are redacted). Wherever possible, BiP will follow good practice by explaining to the data subject that some information has been withheld and why.

Third parties who regularly supply information on staff in a professional capacity (e.g. training course delegates providing feedback forms, etc.) should be informed that anything they submit may become available to the data subject through a Subject Access Request.

Departments should seek consent to disclose at the collection stage (e.g. when requesting references, completion of feedback forms, etc.) to avoid delay upon receipt of a Subject Access Request.

Where professionals request that information supplied by them be kept confidential, they must supply details of the exceptional reasons for making the request. BiP will consider those reasons in order to decide whether they are valid.

Requests for personal data by third parties

Under most circumstances the written consent of individuals must be obtained before disclosing their personal data to third parties.

Disclosure of information about staff: references

All requests for references be handled by Human Resources, where policy is such that very limited personal information is disclosed. This information is limited to what is necessary to verify the details of their employment and role at BiP to a potential employer. In any event, such information will only be disclosed as long as it can be verified that the person making the request:

- is who they claim to be,
- has the authority to make the request and
- has the consent of the applicant.

If in any doubt, seek the consent of the data subject.

It should be noted that data subjects have the right to ask the organisation that receives the reference for a copy of it.

Both organisations and data subjects have the right to take legal action against the authors of references where they consider that the reference has misrepresented the candidate's abilities.

When someone claims legal authority to request personal data

In some cases, requests for personal data may be received from people claiming legal authority to ask for the information concerned. In these cases, recipients of requests should seek advice from the Data Protection Officer.

Unless the person making the request has a warrant or court order requiring BiP to disclose personal information about data subjects, BiP is not obliged to comply with such requests. Therefore, all staff who receive requests for personal data from the police or other government bodies must follow these procedures to ensure that disclosures of personal data are lawful, authorised, and accountable.

All requests for disclosure must be in writing, whether by email or letter. Organisations such as Police Scotland have a standard personal data request form.

Such requests must be signed by an officer with the authority to make the request. This may be an electronic signature or a scanned image of a signed form, if the request is made by email. The name and contact details of the requester and authoriser and the date of each signature must be clear on the form.

The requests must also set out the legal authority for making the request (i.e. specific reference to legislative precedent). The request must explain how this right applies and why they need the information.

Even if the applicant is known to the person handling the request, it is necessary to verify the applicant's identity and their authority to make the request.

Authorising disclosure to third parties

Requests to disclose personal data must be escalated to someone who has the designated authority to decide whether to release or withhold the information.

For requests by the police, Home Office or other government bodies in relation to:

- Customer personal data, the responsible officer is the Data Protection Officer or CIO
- Employee personal data, the responsible officer is the Head of Human Resources, the Data Protection Officer or the CIO.

The responsible officer will need to consider whether:

- The disclosure is necessary for the purpose claimed (e.g. the prevention or detection of crime, or the apprehension or prosecution of offenders);
- Not disclosing the personal data would be likely to prejudice the purpose cited

The responsible officer must be satisfied that the request is reasonable and proportionate and disclose only the minimum personal data necessary for the purpose, seeking advice from the Data Protection Officer as appropriate.

Security of communications

Any and all personal data disclosed in response to a request must be communicated by a method appropriate to the security and sensitivity of the information.

Before supplying information, a check should be made in relation to how the requestor wishes to receive the information and to ensure we have the correct postal or email address.

Information containing sensitive personal data sent by email or using a USB memory stick or other portable media should be encrypted.

If sending a hardcopy, then the packaging should be marked as strictly private and confidential and sent via recorded delivery.

Record retention

It is important that only appropriate information is retained. This reduces the information that may need to be disclosed and so minimises the administrative costs associated with supplying information. It also minimises the risk of reputational damage by ensuring that inappropriate information is not retained.

Audit trail of requests

All subject access requests and requests from third parties must be recorded so that BiP has an audit trail of actions taken in response to a request and can justify each decision. The record must include details of the request, contact details of the applicant, evidence sought and obtained to verify their identity, the decision to release or withhold the information requested, the reasons for the decision and a copy of any information disclosed.

For each disclosure request from the police or government agencies, the following records must also be maintained.

- A copy of the completed police/government agency request form, including the reasons given for the request,
- A record of disclosure decision, recording the decision to withhold or release the information, the information disclosed, where applicable, and reasons for the decision

The recommended retention period for request records is completion plus 6 years in line with that for records that need to be retained for a limited time to defend BiP's legal interests in accordance with the limitations laws of Scotland and the UK.

Guidelines on recording personal information

Staff should observe the following guidelines on recording personal information:

- To be careful about what personal information is retained, including emails
- Wherever possible, limit records to facts
- If recording opinion about someone, it should be justified and supported by substantiating evidence
- Do not record anything you would not wish the data subject to see.

Staff should not hold files on individuals (e.g. staff members). Wherever possible, information should be stored in the appropriate system (e.g. Customer Relationship Management system) or, in the case of information relating to staff, this should be lodged with Human Resources and local copies erased.

Personal data relating to departed staff should be reclaimed from any remote sources and stored in a single location or on a single database, with appropriate security and back-up.

Charges and fees

While the DPA permitted charges for responding to Subject Access Requests, the GDPR requires that access to and rectification or erasure of personal data and the exercise of the right to object is free of charge to data subjects. However, in accordance with the GDPR, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, BiP may either:

- Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- Refuse to act on the request, in which case BiP must demonstrate the manifestly unfounded or excessive character of the request.

Exemptions

Exemptions are an extremely complex part of legislation and must be treated with extreme caution. Anyone dealing with a Subject Access Request, and who thinks an exemption might apply, should contact the Data Protection Officer in the first instance.

Examples in which BiP might be exempt from being required to release information following a Subject Access Request include:

- Data containing information relating to a third party for which consent to release the information cannot be obtained
- Management forecasts such as plans for restructuring, promotions if they would prejudice conduct of business/activity
- Information relating to legal proceedings being taken by BiP against an individual or organisation

For further guidance, please contact the Data Protection Officer.

Policy compliance

If any user is found to have breached this policy, they may be subject to BiP's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). If you do not understand the implications of this policy or how it may apply to you, seek advice from your Line Manager

Review and revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. Policy review will be undertaken by IT.

Appendix 1 – Data subjects' rights

Transparent communication - In order to ensure that personal data are processed fairly, EU data protection law obliges controllers to communicate transparently with data subjects regarding the processing of their personal data.

Exemption where the data subject cannot be identified - Under the GDPR and to the extent that the controller can demonstrate that it is not in a position to identify the data subject, the controller is exempt from the application of the rights of data subjects in Articles 15-22. The controller is also not obliged to obtain further personal data in order to link data in its possession to a data subject.

Time limits for complying with the rights of data subjects - A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of data subjects. If the controller fails to meet this deadline, the data subject may complain to the relevant authority and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months.

Right to basic information - A core principle of EU data protection law is that data subjects should be entitled to a minimum set of information concerning the purposes for which their personal data will be processed.

Right of access - In order to allow data subjects to enforce their data protection rights, EU data protection law obliges controllers to provide data subjects with access to their personal data.

Fees in respect of access requests - The GDPR does not permit such charges in most cases. There is, therefore, an elevated risk that individuals will attempt to exercise these rights merely because they can, or as a cheap but effective means of protest against an organisation.

Right of rectification - Data subjects are entitled to require a controller to rectify any errors in their personal data.

Right to erasure (the "right to be forgotten") - Data subjects have the right to erasure of personal data (the "right to be forgotten") if:

- The data are no longer needed for their original purpose (and no new lawful purpose exists)
- The lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists
- The data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing
- The data have been processed unlawfully
- Erasure is necessary for compliance with EU law or the national law of the relevant Member State.

In essence, the "right to be forgotten" states that data subjects have the right to require an organisation that holds their personal data to delete those data where the retention of those data is not compliant with the requirements of the GDPR. In most cases, provided that an organisation has a lawful basis for processing personal data, it will not be significantly affected by the right to be forgotten.

The right to restrict processing - In some circumstances, data subjects may not be entitled to require the controller to erase their personal data, but may be entitled to limit the purposes for which the controller can process those data (e.g. the exercise or defence of legal claims; protecting the rights of another person or entity; purposes that serve a substantial public interest; or such other purposes as the data subject may consent to). Data subjects have the right to restrict the processing of personal data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:

- the accuracy of the data is contested (and only for as long as it takes to verify that accuracy);
- the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure);
- the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or
- if verification of overriding grounds is pending, in the context of an erasure request.

Notifying third parties regarding rectification, erasure or restriction - Where a controller has disclosed personal data to any third parties, and the data subject has subsequently exercised any of the rights of rectification, erasure or blocking, the controller must notify those third parties of the data subject's exercising of those rights. The controller is exempt from this obligation if it is impossible or would require disproportionate effort. The data subject is also entitled to request information about the identities of those third parties. Where the controller has made the data public, and the data subject exercises these rights, the controller must take reasonable steps (taking costs into account) to inform third parties that the data subject has exercised those rights.

Right of data portability - Data subjects have a right to:

- Receive a copy of their personal data in a structured, commonly used, machine-readable format that supports re-use;
- Transfer their personal data from one controller to another;
- Store their personal data for further personal use on a private device; and
- Have their personal data transmitted directly between controllers without hindrance.

Inferred data and derived data (e.g. a credit score or the outcome of a health assessment) do not fall within the right to data portability, because such data are not "provided by the data subject". In addition, the controller is not obliged to retain personal data for longer than is otherwise necessary, simply to service a potential data portability request.

Right to object to processing - Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data, where the basis for that processing is either public interest, or legitimate interests of the controller. The controller must cease such processing unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or requires the data in order to establish, exercise or defend legal rights.

Right to object to processing for the purposes of direct marketing - Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

Right to object to processing for scientific, historical or statistical purposes - Where personal data are processed for scientific and historical research purposes or statistical purposes, the data subject has the right to object, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Obligation to inform data subjects of the right to object - The right to object to processing of personal data noted above must be communicated to the data subject no later than the time of the first communication with the data subject. This information should be provided clearly and separately from any other information provided to the data subject.

Right to not be evaluated on the basis of automated processing - Data subjects have the right not to be subject to a decision based solely on automated processing which significantly affect them (including profiling). Such processing is permitted where:

- It is necessary for entering into or performing a contract with the data subject provided that appropriate safeguards are in place

- It is authorised by law
- The data subject has explicitly consented and appropriate safeguards are in place.

Document Revision History

Version	Date	Author	Summary
1.0	9 April 2015	Redacted in line with FOIA Sec 40	
2.0	22 September 2017	Redacted in line with FOIA Sec 40	Updated to account for upcoming GDPR.