Global Banking School
+44 (0) 207 539 3548
info@globalbanking.ac.uk
www.globalbanking.ac.uk
891 Greenford Road, London
UB6 0HE

GBS Data Subject Access Request (DSAR) Policy

©2022 Global Banking School

Version Control

Document title: GBS Data Subject Access Request (DSAR) Policy	**No of pages:** 16
Version Number: V2.0	**Date first published:** June 2019
Approved by: Resource Committee	**Last review date:** January 2022
Date originally approved: February 2022	**Due for next review: January 2023**

Related policies
▪ GBS Records Management and Retention Policy ▪ GBS Data Protection Policy ▪ GBS Privacy Policy ▪ GBS Access Control Policy ▪ GBS IT Security Policy ▪ GBS Safeguarding (Prevent) Policy
External Reference
1. Information Commissioner's Office, Accessed online at: https://ico.org.uk/ 2. UK Public General Acts, *Data Protection Act 2018*, Accessed online at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted 3. UK Public General Acts, *Equality Act 2010*, Accessed online at: https://www.legislation.gov.uk/ukpga/2010/15/contents

Contents

Global Banking School Data Subject Access Request (DSAR) Policy

1. Purpose and Scope

1.1 Global Banking School (GBS) needs to collect, store and process personal data about its staff, students, and other individuals it has dealings with, to carry out our functions and activities. GBS is a controller for most of the personal data it processes and is committed to full compliance with the applicable data protection legislation. The Data Protection Act 2018 (DPA) and the United Kingdom General Data Protection Regulation (UK GDPR) gives individuals rights of access to their personal records held by GBS, subject to certain exemptions. This is known as a 'subject access request' (SAR).

1.2 GBS regards the Data Protection Act as an important mechanism in achieving an honest, safe, and open relationship with its students and staff. Requests may be received from members of staff, students, members of the public and any other individual who GBS has had dealings with and holds data. This policy explains how GBS will fulfil its obligations under the Act and provides a guide to staff in dealing with subject access requests that may be received.

2. Role and Responsibilities

2.1 GBS is registered with the Information Commissioner's Officer as a data controller. Details of the school's registration are published on the Information Commissioners website. GBS as a data controller shall implement appropriate technical and organisational measures to ensure that processing of personal information is performed in accordance with the UK GDPR and DPA (2018). Roles and responsibilities include:

2.1.1 Information Commissioner's Office ("ICO"): ICO is the independent regulatory office in charge of upholding information rights in the interest of the public. The organisation covers the Data Protection Act and advises businesses on how to comply with UK GDPR and therefore requires every data controller who is processing personal information to register with the ICO.

2.1.2 Data Protection Officer: DPO is responsible for advising GBS on its obligations, monitoring compliance, assisting with Data Protection Impact Assessments (DPIAs) and liaising with the Information Commissioner's Office. The DPO is also responsible for ensuring that GBS processes the personal information of

its staff, students, customers, providers, and partners in compliance with the applicable data protection rules. Any issues related to Data Protection and compliance issues, please contact dpa@globalbanking.ac.uk.

2.1.3 GBS Academic Standards and Quality Office (ASQO): Responsible for implementation, monitoring and review of this policy and ensuring that training, guidance, and advice regarding data protection compliance is made available to staff and can be contacted on asqo@globalbanking.ac.uk.

2.1.4 Human Resources: Responsible for ensuring that subject access requests (SARs) are processed within one month of receipt in compliance with the ICO's recommendations.

3. Recognising a Subject Access Request (SAR)

3.1 A formal request from a data subject must be made in writing. Please refer to Annex 1 for an example of a Subject Access Request. A request may be made by:

- The person that the data is about (the data subject).
- A representative of the data subject who has their written consent such as a solicitor.

3.2 It is important that all members of staff can recognise that any written request made by a person for their own information is likely to be a valid subject access request. The request does not have to include the words 'subject access' or make any reference to the UK GDPR. A SAR may be a valid request even if it refers to other legislation and should therefore be treated as a SAR in the normal way.

3.3 The person making the request does not have to tell you the reason for making the request or what they intend to do with the information, although it may help us to find the relevant information if they do explain the purpose of the request.

3.4 The following are some of the more common types of requests received:

- 'I would like a copy of all the information you hold about me in my HR file'.
- 'I would like a copy of my student records'.
- 'I am a solicitor acting on behalf of my client and request a copy of their records. A signed authority is enclosed'.

3.5 Requests may sometimes be received from the Police, HMRC or other verified public bodies such as Student Loans Company under for the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax or duty.

3.6 The request should be signed by a Senior Officer from the relevant authority. The request must make it clear that one of the above purposes is being investigated and that not receiving the information would prejudice the investigation.

3.7 In some cases, an individual may mistakenly refer to the "Freedom of Information Act", but this should not prevent GBS from identifying the request as being made under the UK GDPR if appropriate. Some requests may be a combination of a subject access request for personal data under the UK GDPR and a request for information under the Freedom of Information Act 2000 ("FOIA"). Requests for information under the FOIA must be dealt with promptly and in any event within 20 school days.

4. Time Limits and Fees

4.1 Any member of staff who receives a written subject access request must immediately forward it to Human Resources department as the statutory time limit for responding under the UK GDPR is one calendar month from receipt.[1] The timescales for responding do not pause when GBS is closed for holidays, unlike the FOIA.

4.2 A fee may no longer be charged to the individual, student, or staff for provision of this information.[2] Staff processing this request must provide a copy of the information free of charge. However, you can charge a 'reasonable fee' when a request is "manifestly unfounded or excessive", particularly if it is repetitive. GBS may charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that GBS can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information.

4.3 It is advisable for GBS staff to consult any guidance issued by the Information Commissioner's Office (ICO) on what is deemed to be "manifestly unfounded or

[1] *Under the Data Protection Act 2018, Data Controllers previously had 40 calendar days to respond to a request.*
[2] *Previously a fee of £10 could be charged under the Data Protection Act 1998*

excessive" before relying on this exemption, particularly as it is likely to be a high threshold to satisfy.

4.4 GBS in some circumstances may extend the time limit by a further two months if the request is complex or *if* several requests are made from the same individual.

5. Verification

5.1 Staff must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by GBS. The Data Protection Act permits and encourages us to clarify with the requestor what information they need.

5.2 Data subjects must supply their address and valid evidence to prove their identity. GBS accepts the following forms of identification:

- Current UK/EEA Passport (valid)
- UK Photocard Driving Licence (Full or Provisional, valid)
- Firearms Licence / Shotgun Certificate (valid)
- EEA National Identity Card (valid)
- Full UK Paper Driving Licence (valid)
- State Benefits Entitlement Document (past 12 months)
- State Pension Entitlement Document (past 12 months)
- HMRC Tax Credit Document (past 12 months)
- Local Authority Benefit Document (past 12 months)
- State/Local Authority Educational Grant Document or SLC approved documentation (past 12 months)
- HMRC Tax Notification Document (past 12 months)
- Disabled Driver's Pass
- Financial Statement issued by bank, building society or credit card company (past 3 months)
- Judiciary Document such as a Notice of Hearing, Summons or Court Order (past 3 months)
- Utility bill for supply of gas, electric, water or telephone landline (past 3 months)
- Most recent Mortgage Statement (past 12 months)
- Most recent Council Tax Bill/Demand or Statement (past 3 months)
- Current Council Rent Card (past 3 months)
- Current Council Tenancy Agreement (past 12 months)

- Building Society Passbook which shows a transaction in the last 3 months and your address.

6. Processing a Subject Access Request (SAR)

6.1 Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry should be made within GBS' subject access logbook and must include:

- The date of receipt
- The data subject's name
- The name and address of requester (if different)
- The type of data required (e.g., Student Record, Personnel Record)
- The planned date for supplying the information (not more than one calendar month from the request date).

6.2 Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided. (Please refer to Annex 3 to view GBS Subject Access Request Flow Chart).

6.3 By ensuring that the Human Resources department has logged the request, we can ensure that we respond within the statutory timescales. As the time for responding to a request does not stop during the periods when GBS is closed for the holidays. GBS will attempt to mitigate any impact this may have on the rights of data subjects to request access to their data by implementing any necessary measures.

6.4 When responding to a complaint, we must advise the requestor that they may complain to the ICO if they remain unhappy with the outcome.

6.5 If a subject access request is related or may be connected to a disciplinary or grievance for an employee, individual or student, GBS staff should ensure that the broader context is considered when responding to a request and seek advice if required on managing the broader issue and the response to the request.

6.6 Depending on the degree to which information is organised and structured, staff will need to search the following non-exhaustive areas:

- Emails (including archived emails and those that have been deleted but are still recoverable).
- Word documents, spreadsheets, databases, systems.
- CCTV, removable media (for example, memory sticks, floppy disks, CDs)
- Tape recordings, paper records in relevant filing systems etc.

6.7 Staff must not withhold information because they believe it will be misunderstood; instead, they should provide an explanation with the information. Staff must provide the information in an "intelligible form", which includes explaining any codes, acronyms, and complex terms. The information must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. Staff may be able to agree with the requester that they will view the information on screen or inspect files on our premises.

6.8 In some cases, staff must redact any exempt information from the released documents and explain why that information is being withheld.

6.9 Data Subjects have the right to have their inaccurate personal data erased. This is also known as "the right to be forgotten". It is not, however, an absolute right and applies in the circumstances listed below.

6.10 Data Subjects also have the right for inaccurate personal data to be rectified or completed (if it is incomplete). When responding to requests to rectify or delete personal data, staff must process these without undue delay and within one month (using the same procedures as for a SAR). Individuals have the right to have their personal data erased if:

- The personal data is no longer necessary for the purpose for which GBS originally collected or processed.
- GBS is relying on consent as the lawful basis for holding the data, and the person withdraws their consent.
- The personal data has been unlawfully processed.
- GBS is relying on legitimate interest as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing.

6.11 GBS will search databases and other systems and applications where the personal data may be held and erase it within 1 month from the date of the request. In the case of rectifying inaccurate personal data, GBS staff must rectify the information without delay and notify the data subject that this has been completed.

7. Exemptions

7.1 To ensure that people receive only information about themselves, it is essential that a formal system of requests is in place. Certain information may be exempt from disclosure so GBS staff must consider the below exemptions and decide whether these can be relied upon.

7.2 In practice, this means that GBS staff may be entitled to withhold some documents entirely or may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. The exemptions are set out in Schedules 2 and 3 of the DPA 2018 and these include:

- Crime and taxation: general
- Crime and taxation: risk assessment
- Legal professional privilege
- Functions designed to protect the public
- Regulatory functions relating to legal services, the health service and children's services
- Other regulatory functions
- Judicial appointments, independence, and proceedings
- Journalism, academia, art and literature
- Research and statistics
- Archiving in the public interest
- Health, education, and social work data
- Child abuse data
- Management information
- Negotiations with the requester
- Confidential references
- Exam scripts and exam marks
- Other exemptions

7.3 Where an exemption applies, GBS may refuse to provide all or some of the requested

information, depending on the circumstances. GBS can also refuse to comply with a SAR if it is 'manifestly unfounded or manifestly excessive'. If GBS refuses to comply with a request, the individual must be informed of:

- The reasons why.
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through the courts.

7.4 If a request involves information about other individuals, GBS will consider whether it is possible to comply with the request without disclosing information that identifies another individual. If this is not possible, GBS does not have to comply with the request except where the other individual consents to the disclosure or it is reasonable to comply with the request without that individual's consent.

7.5 Data on a deceased person is confidential however it is not covered by the Data Protection Act but instead by the Freedom of Information Act. In deciding whether to allow access to an individual requesting information in relation to a deceased person staff will need to consider any responsibility of confidentiality to that deceased person. Staff should also consider the rights of the data subject under the Human Rights Act, Article 8 - the right to respect for a private and family life.

8. Guidance for Communications/Response to SAR

8.1 All correspondence must include the following information:

- The purposes of the processing.
- Categories of personal data concerned.
- The recipients or categories of recipients to whom personal data has been or will be disclosed, in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or model clauses.
- Where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period.
- The existence of 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.
- The right to lodge a complaint with the supervisory authority, the ICO.
- If the data has not been collected from the data subject: the source of such data.

- The existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

9. Related policies/Review

9.1 Reference should also be made to GBS Data Protection Policy, GBS Privacy Policy, GBS Records Management and Retention Policy. Information on other related policies is available from GBS Academic Standards and Quality Office (ASQO) and can be found under the GBS General Policies folder on SharePoint.

9.2 This policy is subject to review and can be amended by GBS at any time and updated in accordance with government legislation.

10. Alternative Format

10.1 This policy can be provided in alternative formats (including large print, audio and electronic) upon request. For further information, or to make a request, please contact:

- **Name:** Welfare Management Team
- **Position:** Welfare Officer/Manager
- **Email:** welfare@globalbanking.ac.uk

Annex 1- Example of a Subject Access Request

[Name and address of the organisation]

[Your name and full postal address]

[Your contact number]

[Your email address]

[The date]

Dear Sir or Madam

Subject access request

[Include your full name and other relevant details to help identify you].

Please supply the personal data you hold about me, which I am entitled to receive under data protection law, held in:

[Give specific details of where to search for the personal data you want, for example:

- my personnel file;
- emails between 'person A' and 'person B' (from 1 June 2017 to 1 Sept 2017)
- my medical records (between 2014 and 2017) held by 'Dr C' at 'hospital D';
- the CCTV camera situated at ('location E') on 23 May 2017 between 11am and 5pm; and
- financial statements (between 2013 and 2017) held in account number xxxxx.]

If you need any more information, please let me know as soon as possible.

[If relevant, state whether you would prefer to receive the data in a particular electronic format, or printed out].

It may be helpful for you to know that data protection law requires you to respond to a request for personal data within one calendar month.

If you do not normally deal with these requests, please pass this letter to your data protection officer or relevant staff member.

If you need advice on dealing with this request, the Information Commissioner's Office can assist you. Its website is ico.org.uk, or it can be contacted on 0303 123 1113.

Yours faithfully

[Signature]

Please note, the above subject access request example was obtained from the ICO website.

Annex 2- Glossary

Subject Access Request or SAR A request for access to data by a living person under the Act is known as a Subject Access Request or SAR. All records that contain the personal data of the subject will be made available, subject to certain exemptions.

Freedom of Information Request or FOI. A request for access to data held is dealt with under the Freedom of Information Act 2000 and is known as a Freedom of Information Request or FOI. Requests for the data of deceased people may be processed under this legislation.

Personal Data Personal data means data which relate to a living individual who can be identified directly or indirectly from the data, particularly be reference to an identifier. Personal data can be factual (such as a name, address, or date of birth) or it can be an opinion (such as a performance appraisal).

Special Category Data Certain personal data, special category data, is given special protections under the Act because misuse could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Special category data includes: a person's racial or ethnic origin; political opinions; religious or similar beliefs; trade union membership; physical or mental health or condition or sexual life; biometric or genetic data.

Data Controller The organisation which determines the purposes and the way, any personal data is processed is known as the data controller. GBS is the data controller of all personal data used and held within each individual department.

Data Processors Organisations or individuals who process personal data on behalf of a data controller are known as data processors.

Data Subject A living identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Protection Officer A Data Protection Officer ensures that GBS processes the personal data of its staff, students or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

Information Commissioner's Office ("ICO") ICO is the independent regulatory office in charge of upholding information rights in the interest of the public.

Breach any act or omission that compromises the security, confidentiality, integrity or availability of personal data.

Annex 3- GBS Subject Access Request Flow Chart