POLICY & GUIDELINES

BMI Group Internal Guidelines For Managing Data Subject Access Requests

Effective: June 16, 2022

1. Purpose of these internal guidelines

Under the General Data Protection Regulation (“GDPR”), data subjects have the right to receive information regarding the personal data that BMI Group or any of its group companies as data controllers (“BMI”) holds about them and also to receive a copy of that data. These internal guidelines are intended to support the BMI team involved in dealing with data subject access requests (“DSAR”), which will typically be HR, Finance, IT and Legal. To the extent that legislation in your local jurisdiction applies, the definitions used and referred to in these guidelines, and any analogous terms shall have the means and definitions set out in the respective local legislation.

For the purposes of these guidelines, "personal data" means any information relating to an identified or identifiable natural person, and in the event that the Protection of Personal Information Act 4 of 2013 ("POPIA") applies, an identifiable, existing juristic person ("Data Subject"). An identifiable natural person and/or juristic person (where applicable) is one who can be identified, directly or indirectly, by reference to an identifier, such as name, identification number, registration number (where applicable) or online identifier such as an IP address.

The categories of individuals from whom we are most likely to receive a DSAR are unsuccessful candidates, employees, former employees and customers. DSARs, however, can be made by anyone who wants to find out if BMI processes their personal data and BMI may receive opportunistic requests from people simply looking to put us through the effort of responding to the request.

Unless otherwise directed by Group Legal, HR (or those with HR responsibility where local

country teams do not have a specific HR point of contact) will be responsible for managing and responding to DSARs which relate to employees or former employees and Finance will be responsible for dealing with requests from customers (referred to in these Guidelines as the “Responding Team”).

2. Receipt of DSARs and Request Form

All Company employees, temporary staff, contractors, and consultants (“User”) wherever located, are expected to comply with this Policy.

3. Managing a DSAR request

Timing

Under GDPR, we are required to respond to DSARs within one month. The Responding Team should respond to acknowledge receipt of the request as soon as possible after receipt. In some cases this response may include request for clarification (see below). The one month period begins once we receive: (i) the request; (ii) evidence of the Data Subject’s identity (see below); and (iii) a response to clarification requests that we may make after receiving the request (see below).

If the request is complex it is possible to extend the timeframe for response to three months.

Whether a response can be regarded as “complex” depends on a number of factors such as how many systems need to be searched and how many documents are

returned. Approval should be obtained from Group Legal before communicating to a Data Subject that their request is complex and that BMI’s response timeframe will be extended in line with GDPR. If the timeframe will be extended, this needs to be confirmed to the Data Subject within one month of them making the request and the reasons why the request is complex need to be set out.

To limit the risk of disputes around whether the response has been provided on time, records should be kept of each step in the process. We have created a tracker spreadsheet (available on Google Sheets at this link) which tracks information such as: (i) the date the request was made (whether via the *dsar@bmigroup.com* address or otherwise); (ii) the date an extension to the timeframe for responding was communicated (if applicable); (iii) the date we are treating the timeframe for response as starting. The format of the table is set out in Appendix 2.

Clarifying a request

Requests for “all of my personal data” are difficult to manage and would require us to search a wide variety of systems where we may hold information relating to a Data Subject.

This is why BMI seeks to encourage Data Subjects to be specific in their DSAR in the form that we have created, and where applicable in the form prescribed under applicable local legislation

If we receive a request which does not give any specifics such as the topic, date ranges or systems that the Data Subject would like us to search, we can seek clarification of their request. For example, we may ask if they are looking to access their personal data relating to a specific event, topic or timeframe.

If the Data Subject is unwilling to be more specific it is likely to impact the timeframe for response as a wide search is likely to return large volumes of data that we will need to

review to identify their personal data (see above).

Confirming the identity of the Data Subject

We require Data Subjects to prove their identity before we can respond to a request. This is made clear in the request form mentioned above. If we receive requests via means other than the Company form via *dsar@bmigroup.com*, we will need to obtain proof of identity from the Data Subject.

To prove identity we require: (i) a photocopy or a scanned image of a passport or photo identification such as a driver's license or national identification number card; and (ii) a copy of a bank or credit card statement or utility bill showing the Data Subject's current address and dated within the last three months. Any personal data that is collected in order to identify the Data Subject must be retained for no longer than necessary for the purposes for which it was obtained. For example, for customers who make a DSAR and for whom we do no hold a passport on file for any other purpose, in most circumstances we should destroy any hard copies of the passport and delete any electronic copies within three months of responding to the DSAR (but keeping a record of the fact that we carried out the appropriate identify checks).

In some instances we may waive the requirement to prove identification, for example, if the request is made by an existing employee and is made directly to the HR team. Any decisions to waive the requirement must be approved by Group Legal.

Form of the response and language of the response

We should provide the Data Subject with a copy of the personal data processed by us in a commonly used electronic form such as pdf (unless the Data Subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form).

Any correspondence to the Data Subject should be in the same language in which they made the request. If the personal data which is identified as a result of the searches is in another language than the one in which the request was made, this can be provided to the Data Subject in its original language. For example if there is an email between the Data Subject and a colleague in English but the Data Subject is a Polish employee and has made the request in Polish, we can provide them with the relevant part of the email which contains their personal data in English.

Fees

Under GDPR we cannot charge for responding to a DSAR. There are limited exceptions to this, including if the Data Subject asks for further copies of the information that we send them, when we can make a reasonable charge. In theory under GDPR we can also charge a reasonable fee for "repetitive requests" and "manifestly unfounded or excessive requests". In practice it is unlikely that we will be able to rely on those latter exceptions. Approval must be given by Group Legal before any fees are communicated or charged to the Data Subject making the request.

In the event that POPIA is applicable, we may charge a fee for responding to a DSAR. The fees applicable to DSAR's under POPIA are set out in Appendix 5 - POPIA DSAR Fees." We have attached a document titled POPIA DSAR Fees which contains the fees applicable to DSARs under POPIA.

Rights of other Data Subjects

GDPR recognises that subject access requests may adversely affect the rights of others, such as individuals whose personal data we hold and a company's trade secrets.

A Data Subject is only entitled to personal data relating to them and we should not provide any data that adversely affects the rights of others. This means that we should not divulge personal data relating to other Data Subjects. For example, if an email includes a list of employees with their bonus awards, we should not send information relating to the other employees' bonuses (or even the other employees' names or other information by which they could be identified) to the individual making the request.

4. Practicalities of searches

The Responding Team will need to work closely with their local IT teams to respond to a request. IT should be informed about the request as soon as practicable after it is received (and even if we are at a stage where we are seeking clarification of the request) so that they can allocate resources to support with the searches.

Where to carry out the searches

Where IT carries out the searches will depend on what information the Data Subject has requested access to. You will find a list below of examples of the locations where personal data may be held. The exact systems will vary according to the different countries in which BMI operates and the entities which is/are the data controller(s). You may not need to search every type of system for every case, depending on what the Data Subject has requested.

- Laptop/PC
- Mobile devices
- Tablet devices
- Email (Gmail), including legacy systems (Microsoft Outlook/Lotus Notes)
- Network shares
- Sharepoint/G-Drive
- HR Systems
- Expense report systems
- Time cards (physical & virtual)
- Physical files

Company searches must be conducted in accordance with the BMI Acceptable Use Policy, in particular as it relates to any legitimate expectation of privacy that a BMI employee may have regarding their communications (whether on company devices or systems or on personal devices) per local law. For example, in France if an email is marked "Private" then an employee has an expectation of privacy in relation to that email and they should not be accessed unless approval is given by Group Legal.

What search terms to use

The search terms that are used will also be determined by the request itself. In Appendix 4 we have set out examples of requests which we anticipate may be made and have included suggested search terms. These terms are not intended to be an exhaustive list and HR should consider if there are other appropriate words that should be searched in relation to each request.

Communicating approach with the Data Subject

Once the locations for the search and the search terms have been identified, it is good practice to write to the Data Subject to confirm the basis on which the search will be carried out. This can avoid a situation where the request is finalized and then the Data Subject challenges the basis on which the search has been carried out.

5. Preparing the response

As mentioned above, we need to be mindful of the rights of other Data Subjects. This means that the personal data of the Data Subject making the request may need to be extracted from the search results or redacted so that we only provide the Data Subject with their own personal data. For example, in an email which sets out bonus awards for a number of employees, we could extract the information relating to the Data Subject's bonus and include it in a table (see example in Appendix 4). Some documents will only include information relating to the Data Subject and can be sent to the Data Subject in their entirely without extraction or redaction, for example performance review forms or letters confirming a pay increase.

Redaction can lead to more questions from the Data Subject about what information has been deleted, as the Data Subject has the benefit of seeing the document. On that basis in most instances it will be preferable to extract the information unless the volume of information makes that impractical.

If sending the personal data electronically (which will be required if the request was received in electronic format), the file should be password protected or encrypted (where encryption resources are available)

6. Responding to the request

In addition to sending the information that has been collated, we also have to provide the Data Subject with the following information:

(a) the purposes for the processing of the personal data we hold;

(b) the categories of personal data concerned (for example, contact details, bank account information and details of sales activity);

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas (for example, US-based service providers);

(d) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;

(e) the right to lodge a complaint with the local data protection authority in their country (or region, if applicable);

(f) where the personal data are not collected from the data subject, any available information as to their source;

(g) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(h) the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and

(i) where personal data are transferred outside the EU, details of the

appropriate safeguards to protect the personal data.

Template letters will be made available by Group Legal to use as the starting point for BMI's response.

7. Other rights of Data Subjects under GDPR

In addition to the right to access which is dealt with in this guidance, there are other rights for Data Subjects which are set out in GDPR. In particular the right to rectification, the right to restriction, the right to portability, the right to erasure and the right to object to processing. These rights are explained further in BMI's Privacy Policies.

In many cases these rights are not absolute, for example, if a former employee requests that we delete all of their personal data, BMI has the right to explain that it cannot delete all of the personal data as there is a requirement for BMI to keep some personal data to comply with its legal obligations (e.g.,BMI has a legal obligation to keep tax records for specified periods (according to local laws)).

In the event that a Data Subject makes one of these requests, they should be forwarded to privacy@standardindustries.com and Group Legal will help determine the appropriate response

7. Changes to these Guidelines

These DSAR guidelines will be reviewed and updated as necessary by Group Legal. Any questions relating to the Guidelines should also be directed to Group Legal.

APPENDIX 1 - Subject Access Request Form

Under the General Data Protection Regulation (GDPR), you have the right to access your personal data held by companies within the BMI Group who act as data controllers (i.e. those which make decisions about why and how your personal data is processed). If you wish to obtain this information, you should submit this form and evidence of your identity via email to dsar@bmigroup.com or to your local HR team if you are an existing employee.

We typically expect to respond to your request within one month of receipt of a fully completed form, proof of identity and receipt of any information we have requested from you to clarify your request. However, if the request that you make is complex, we may extend the timeframe and respond within three months. We will inform you if we need to extend the timeframe.

Requester Name (Data Subject) and Contact Information

We will only use the information you provide on this form to identify you and the personal data you are requesting access to, and to respond to your request.

Surname	
First name(s)	
Date of birth	

Address	
Email	
Phone number	

Connection with BMI Group

Please tick the box below that relates to you and complete the requested information.

Current employee	State name of your employer
Former employee	State name of former employer
Customer	State customer account numbers (if known) or confirm name of supplier companies

Other	Please state connection

Information Requested

To help us process your request, please provide as much detail as possible about the personal data you are requesting access to in the box below. For example, if you are a current or former employee you might be asking for access to personal data relating to a particular event such as promotion or training records or if you are a customer you might want to access information relating to your purchase history. Other information that will help us to conduct the search will include references to date ranges and the type of documents that you would like to search.

We will contact you for additional information if the scope of your request is unclear or does not provide sufficient information for us to conduct a search.

Surname	
First name(s)	
Date of birth	
Address	
Email	
Phone number	

Please be aware that GDPR recognises that subject access requests may adversely affect the rights of others, such as individuals whose personal data we hold and a company's trade secrets. When we respond to your request we will do so in a way that does not adversely affect such rights. This may mean that we provide you with extracts of information which include your personal data or redact documents, as appropriate.

Proof of Data Subject's Identity

We require proof of your identity before we can respond to your access request. To help us establish your identity, you must provide identification that clearly shows your name, date of birth, and current address. We reserve the right to refuse to act on your request if we are unable to identify you.

We will accept a photocopy or a scanned image of one of the following as proof of identity: passport or photo identification such as a driver's license or national identification number card. If you have changed your name, please provide the relevant documents evidencing the change. Please also attach a copy of a bank or credit card statement or utility bill showing your current address and dated within the last three months.

If you do not have any of these forms of identification available, please contact us via dsar@bmigroup.com for advice on other acceptable forms of identification.

Signature and Acknowledgement

I confirm that the information provided on this form is correct and that I am the person whose name appears on this form.

I understand that BMI Group may need to contact me again for further information and that my request will not be valid until BMI Group receives all of the required information to process the request.

_____

_____ Signature

_____

_____ Date

APPENDIX 2 - Format of BMI Group DSAR Tracker form

Receipt of request. Note: 1) **Name of Data Subject;** 2) **date request received; 3) date for response (one month from this date if have identify of Data Subject and request sufficiently clear)**	**Date acknowledgment of response sent (including any requests for clarification if appliacable)**	**Date clarification received (timeframe for response starts on this date)**	**Locations for search**	**Search terms**	**Date response sent**	**Details of any follow up communication from Data Subject**

APPENDIX 3 - Examples of potential requests and search terms

These scenarios are examples and should be used as a guide only. Our response process will change depending on the nature of each request we receive. The Responding Team should consider each request on a case by case basis.

The search terms suggested are not intended to be an exhaustive list and the Responding Team should consider if there are other appropriate words that should be searched in relation to each request.

Example 1

A former employee makes a DSAR request using the DSAR form, and submits the completed form to dsar@bmigroup.com. The former employee has requested all information in relation to a claim for compensation that they made during their employment at BMI Group. The completed form is forwarded to HR from the internal mailbox:

1. Complete the Google Sheet and fill out the details of the request.
2. You have one month from receiving the request to respond. Diarise and prioritise accordingly.
3. Confirm the relationship of the data subject to BMI and decide if BMI is responsible for processing of "personal data" of the data subject.
    - In this case, as the request has come from a former employee, BMI would control and process personal data of the data subject, including name, address, location data and potentially other sensitive information, and for payroll purposes.
4. Confirm the identity of the data subject BMI.
    - If the identification is sufficient to determine the identity of the data subject, proceed to answer the request. See "Confirming the identity of the Data Subject", in the DSAR Guidelines.
    - If the identification provided is insufficient to determine the identity of the data subject, respond to the data request and ask the data subject to provide sufficient identification.
    - Any decisions to waive the requirement must be approved by Group Legal.
5. Search all paper records and relevant storage units, e-mail systems, computer drives, or other systems, to locate any relevant information (see "*Where to carry out the searches", in the DSAR Guidelines).* If necessary, extend the request to the appropriate team manager.

    Search terms would include the following:

    - Always search the following: full name, first initial and surname and initials; **and**
    - Case specific terms will be needed to narrow the search. In this case, it could include: compensation, payment, reimbursement.

Example 2

A current employee emails you as their HR manager. They tell you that they are making a "personal data information request" and would like to receive all of the data that BMI holds in relation to their salary.

1. Even though the request has not come through to the central mailbox using the form, it is still a valid DSAR request under the GDPR and should be managed by HR as the request is from an employee.
2. You should complete the Google Sheet and fill out the details of the request.
3. You have one month from receiving the request to respond. Diarise and prioritise accordingly.
4. Confirm the relationship of the data subject to BMI and decide if BMI is responsible for processing of "personal data" of the data subject.
    - As a current employee, BMI controls and processes personal data of the data subject.
5. Confirm the identity of the data subject.
    - Given the data subject is a current employee, we should be able to answer this question without requesting further identification and can proceed to answer the request.
6. Search all paper records and relevant storage units, e-mail systems, computer drives, or other systems, to locate any relevant information (see "*Where to carry out the searches*", above). If necessary, extend the request to the appropriate team manager.

    Search terms would include the following:

    - Always: full name, first initial and surname and initials; **and**
    - Case specific: Where we receive a request relating to salary or performance, need to search for both Compensation (search terms include: salary, payment, benefit, reward, pay, income, wage remuneration) and , Performance (search terms include: KPI, objectives, achievement, behaviour, capability, competence, ability, review, bonus, performance, appraisal, evaluation, assessment).

Example 3

A former employee sends a completed DSAR request form to the central mailbox. They note they were made redundant and want "all information that BMI has about me". The request will be forwarded to HR as the team responsible for managing requests from former employees.

1. You should complete the Google Sheet and fill out the details of the request.
2. You have one month from receiving the request to respond. Diarise and prioritise accordingly.
3. Confirm the relationship of the data subject to BMI and decide if BMI is responsible for processing of "personal data" of the data subject.
    - It is important to confirm the data subject was a former employee of BMI. You may need to use the identification provided. If the data subject was a former

employee, BMI would control and process their personal data and we should proceed to respond to the request.

4. Confirm the identity of the data subject.
    - If the identification is sufficient to determine the identity of the data subject, proceed to answer the request. See "*Confirming the identity of the Data Subject", above.*
    - If the identification provided is insufficient to determine the identity of the data subject, respond to the data request and ask the data subject to provide sufficient identification.
    - Any decisions to waive the requirement must be approved by Group Legal.
5. This request is very wide and will be difficult to manage practically. In this instance, the request may be too broad to respond to at this point because of the breadth of information requested.
    - Approval should be obtained from Group Legal before communicating to a Data Subject that their request is complex and that BMI's response timeframe will be extended in line with GDPR. Group Legal will assist with the handling of the request for clarification.
    - If the timeframe will be extended, this needs to be confirmed to the Data Subject within one month of them making the request and the reasons why the request is complex need to be set out.
6. Search terms could include the following:
    - Always: full name, first initial and surname and initials; **and**
    - Case specific: should search for Compensation (search terms include: salary, payment, benefit, reward, pay, income, wage remuneration), Performance (search terms include: KPI, objectives, achievement, behaviour, capability, competence, ability, review, bonus, performance, appraisal, evaluation, assessment), and Redundancy (search terms include dismissal, termination, resignation, discharge, tenure, contract).

Example 4

A potential customer makes a DSAR request which is forwarded to Finance as the team ordinarily responsible for dealing with customer requests. The customer was looking to purchase BMI product but did not proceed. The request asks for "personal data that BMI has about me."

1. You should complete the Google Sheet and fill out the details of the request.
2. Confirm the relationship of the data subject to BMI and decide if BMI is responsible for processing of "personal data" of the data subject.
    - In this case, we may not be processing any information about the data subject.
    - However, processing is a broad term, and includes storing the information. It also includes obtaining information which it is intended will be stored as personal data.
    - If you are unsure, contact Group Legal for assistance.
3. Once you have engaged Group Legal and have determined that BMI does process personal data of the data subject, we can proceed to respond. You should complete the Google Sheet

and fill out the details of the request. If you do not think that BMI processes personal data of the data subject, approval should be obtained from Group Legal before communicating to a Data Subject.

4. You have one month from receiving the request to respond. Diarise and prioritise accordingly.
5. Confirm the identity of the data subject.
    - If the identification is sufficient to determine the identity of the data subject, proceed to answer the request. See "*Confirming the identity of the Data Subject", above.*
    - If the identification provided is insufficient to determine the identity, respond to the data request and ask the data subject to provide sufficient identification.
    - Any decisions to waive the requirement must be approved by Group Legal.
6. This request is very wide and will be difficult to manage practically. In this instance, the request may be too broad to respond to at this point because of the breadth of information requested.
    - Approval should be obtained from Group Legal before communicating that further specifics or information is required from the data subject. Group Legal will assist with the handling of the request for clarification.
    - If the timeframe will be extended, this needs to be confirmed to the Data Subject within one month of them making the request.
7. Search terms could include the following:
    - Always: full name, first initial and surname and initials; **and**
    - Case specific: should search for the product name and type (current and previous) and could be narrowed by date.

APPENDIX 4 - Extraction of Personal

Internal note: Under GDPR we have to inform the Data Subject of the recipients or categories of recipient to whom the personal data has been or will be disclosed. Separating out the location of the personal data in this way helps us achieve that requirement.

Internal emails between Data Subject and BMI Group employees

Personal Data	**Date**
"Based on his achievement against personal objectives, Jane Smith is awarded a bonus of £5,000 for FY2017"	3 January 2018

External emails between BMI Group entity and external recipients

Personal Data	**Category of Recipient**	**Date**
"We have recently recruited Jane Smith. Please set her up in the payroll system with an annual salary of £60,000"	Payroll provider	18 May 2010
"Please enrol Jane Smith in the pension plan starting 1 June 2010 with employee contributions of 5% and company contributions of 5%"	Third party benefits provider	20 May 2010

The Responding Team should consider if other categories of document from which personal data has been extracted should be included, for example word files, Google documents, excel spreadsheets or PowerPoint presentations.

[1] The upload of these forms to local websites and intranets of BMI Group companies is in progress.