navitas

transforming lives through education

UPE and GSM Data Subject Rights Procedure

K. Marshman
04/2024

UPE & GSM Data Subject Rights Procedure

Navitas Pty Limited
ACN 109 613 309

Document

Document Name	UPE & GSM Data Subject Rights Procedure
Responsibility	Global Head of Data Privacy
Initial Issue Date	04/2024 Version 1

Version Control

Date	Version No.	Summary of Changes	Reviewer Name and Department/Office
15/11/2023	0.1	Initial Draft	K. Marshman - Privacy
01/12/2023	0.2	Amendments	K. Marshman - Privacy
14/12/2023	0.3	Additions for PIPEDA	E. Scrivens – PrivacyWorks
04/01/2024	0.4	Additions	K. Marshman - Privacy
09/01/2024	0.5	Additions	H. Selby – Privacy
02/04/2024	1	Final	K. Marshman - Privacy

navitas

transforming lives through education

1. Contents

2. Introduction

This procedure sets out the process and responsibilities of the UPE and GSM divisions on answering individual rights under the EU GDPR, and any relevant local privacy legislation.

Individual Rights are included in almost all privacy legislation. The EU GDPR has the most individual rights, but common ones are the Right of Access (a right to request a copy of the personal information a company holds on you) or a right to Erasure (the right to ask a company to delete personal data it holds on you).

This Procedures explains how to manage individual rights requests, from the initial request being received, through to sending a response and managing any appeals resulting from the requester being unsatisfied with the results.

3. Purpose & Scope

The main purpose of this procedure is to govern the way in which individual rights are processed, and whose responsibility it is to complete each part of that process. The main audience will be the divisional privacy teams, but all employees of Navitas are required to understand this procedure and work within its requirements.

This Procedure applies to University Partnership Europe and the Global Sales and Marketing Division. In the event GSM local privacy legislation differs from the EU GDPR, local legal obligations will need to be assessed and met. However, any data subject rights under the EU GDPR will be honoured globally at Navitas and its Colleges.

4. Responsibilities

4.1 Global Head of Data Privacy & DPO or Global Privacy Manager & Deputy DPO

- Serve as the main point of contact for Supervisory Authorities/Regulators for Data Subject Rights
- Cooperate with Supervisory Authorities/Regulators.
- Monitor compliance with Data Subject Rights, including awareness raising and training, audits, and assignment of tasks.
- Responsible for providing reporting to senior management to ensure visibility and accountability of Data Subject Rights.
- Continuously report on progress and mitigation of privacy risks.
- Lead the Privacy Team to ensure the best possible privacy compliance across the business.

4.2 Divisional Privacy Managers

- Logging and managing requests
- Providing advice, in collaboration with the Global Privacy Team

- Gaining reasonable ID and asking for clarification where required.
- Application of exemptions, in collaboration with Global Privacy Team
- Responding to complaints

4.3 Heads of Departments and Managers

- Responsible for promoting this policy, and associated procedures to their team members.
- Responsible for the upkeep of their department RoPA entries and responding to update requests from the Privacy Team.
- Responsible for adopting the Privacy by Design and Default approach within their areas
- Responsible for asking the Privacy Team for guidance as and when required

4.4 Navitas employees and any third parties who have access to Navitas personal data

- Are responsible to adhering to this policy and associated procedures
- Asking for help and advice whenever needed
- Protecting the personal data they are entrusted with
- Recognising Data Subject Rights requests and following the agreed process

5. What are data subject rights?

The Data Subject Rights are below. A more detailed description of these can be found in the Data Subject Rights Guidance, you can follow this link.

- Right to be Informed
- Right of Access
- Right to Rectification
- Eight to Erasure
- Right to Restriction of Processing
- Notification Obligation
- Right to Data Portability
- Right to Object
- Automated decision making, including profiling.

Other Privacy legislation may have different, additional or less individual rights than the EU GDPR and it is the responsibility of the Divisional Privacy Manager to access which privacy legislation is engaged. However, due to Navitas adopting the EU GDPR globally, no matter where the personal data is processed, or the reach of local privacy laws, any individual rights under the EU GDPR will be honored.

6. Identifying a Request

If a data subject rights request is received out in the business, anywhere globally, the following explains what action to take.

Verbal request – Verbally accept the request by return. Then ask for an email address or other way of contacting them. Send this information, along with the date and time of the verbal request, to the privacy team at privacy@navitas.com. The Divisional Privacy Manager will then be responsible for picking up the request and managing it from there.

Email requests – Immediately forward the request onto privacy@navitas.com. Nothing else is required, no acknowledgement or receipt of the request is needed, this will be managed by the Divisional Privacy Manager.

Postal requests – Scan the letter, if possible (or photograph with phone) and send through to privacy@navitas.com along with a date if not detailed on the letter. The date is required to be the date Navitas receives the letter, not the date it is sent through to the Privacy Team, so it is vital it is sent through on the day it is received.

Social media requests – As with verbal requests, social media requests should be accepted via that channel. However, instead of asking for an email address to contact them on (this would be asking them to publish their personal details online) provide them with the privacy@navitas.com email address and ask them to contact the privacy team to move their request forward. Then ensure you follow up directly with the Divisional Privacy Managers on privacy@navitas.com to let them know, so they can follow up.

7. Verifying the identity of the requestor

Navitas must verify the identity of the person making the request, using 'reasonable means'. It is vital to not send personal data about one individual to the wrong person, or to delete, rectify personal data of the wrong individual, depending on their request type. This can happen either accidentally or because of deception, if Navitas has not confirmed the identity of the requester.

Identification is to be sought in the following ways and is the responsibility of the Divisional Privacy Manager.

Navitas employees

An email from a Navitas.com email address will suffice as "reasonable." The use of a Navitas email means that the employee has already gained access to their Navitas account and provided a correct password. Employees are also subject to the Navitas Acceptable Use Policy. If they do not wish to use their Navitas email account to make their request, the process below for everyone else will be engaged.

Everyone else

A request from someone who does not have a Navitas account must be able to provide "reasonable" proof they are who they say they are. One Form of Photo ID is preferable, but other forms of ID are acceptable. ID accepted are as follows.

- Copy of passport
- Copy of visa (for international students)
- Copy of driving license
- Copy of birth certificate

If one of the above is not available, the Divisional Privacy Manager is responsible for talking with the requester and deciding on an appropriate alternative, such as non-photographic identification. Items accepted include;

- Bank statement
- Energy Bill
- Mobile Bill

The name of the requester needs to be on the document, and it needs to be within 6 months old.

Should no form of identity be available, the divisional privacy manager will speak with the global privacy team for advice.

The Divisional Privacy Manager is also responsible for noticing any irregularities which may indicate someone pretending to be the individual is trying to make a request without authorisation. In these instances, the request is to be brought to the attention of the DPO immediately. A decision on the way forward will be decided jointly, with seniority on a decision falling to the DPO.

8. Requests made on behalf of others

Requests can be made on behalf of others if the appropriate ID and Authorisation are provided.

ID needs to be gained for both the party whose personal data forms the request, and from the individual making the request on their behalf. Authorisation is also required from the individual whose personal data the request relates to, which explicitly confirms they are happy for the other individual to make it for them.

ID will be required of the individual the request is based on, and the individual making the request on their behalf. Additional to the two sets of ID, there is a need to provide authorisation from the individual (not the requester) which gives permission for the requester to act on their behalf.

9. Charging for information

Navitas will provide a copy of the information free of charge, with the exception that we can charge a ‘reasonable fee’ when a request is ‘manifestly unfounded or excessive’, particularly if it is repetitive.

We may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that we can charge for all subsequent access requests.

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

A charge should not be made without the prior agreement of the Global Team.

10. Request deadlines

Information must be provided without delay and at the latest within:

- one month of receipt for standard requests.

The one month response is a legal deadline, and the time to answer will begin at the point a valid request (which includes a valid form of ID) is received.

Any extensions to the one month deadline come with a requirement to keep the requester fully informed with progress via regular updates.

Authorisation for extension is required from the Global Team. It is important to acknowledge that staff shortages are not a reason to extend to the 2-month deadline, and any requests as such will be refused.

11. Processing the Request

Since data subject requests are a legal right, they are to be processed and managed by the Divisional Privacy Manager. In the unlikely event of a large volume of requests, other Divisional Privacy Managers are available to assist.

There is a one month deadline to respond to requests. This is required whether the request can be actioned, or not. Template response letters are to be used in all circumstances. These can be found on the Privacy SharePoint site.

All requests will be acknowledged within 2 days of receipt, However, all efforts should be made to send an acknowledgement on the day of the request arriving. If clarification is required, this should be sent to the requester within five working days receipt of the request, no longer. However, where possible, clarification should be sent with the acknowledgement.

Depending on what lawful basis the personal data is being processed under, will depend on the response to data subject rights. The below table provides information on what Rights are engaged depending on the lawful basis used.

For example, if a student puts a right of erasure request in, but we are processing that personal data under “legal obligation” then the response will be an explanation of which we cannot erase their personal data. However, if we get a request for the right to object and the lawful basis is “legitimate interests” then that right would be engaged.

Right of the data subject	Consent	Contract	Legal Obligation	Vital interests	Public interest	Legitimate interest
Withdraw consent	Yes	No	No	No	No	No
Be informed	Yes	Yes	Yes	Yes	Yes	Yes
Access	Yes	Yes	Yes	Yes	Yes	Yes
Rectification	Yes	Yes	Yes	Yes	Yes	Yes
Erasure	Yes	No	No	No	No	Yes
Restrict processing	Yes	Yes	Yes	Yes	Yes	Yes
Data portability	Yes	Yes	No	No	No	No
Object	N/A	No	No	No	Yes	Yes
Automated decision making and profiling	N/A	No	No	Yes	Yes	Yes

12. Searching and gathering the requested information

Once the Divisional Privacy Manager has logged and acknowledged the request, they will then contact the relevant department or college for the personal data requested.

It is the responsibility of the department or college which holds the personal data to gather it and send it, securely, to the divisional privacy manager upon request. This should be done within 5 working days, unless the request is particularly burdensome.

Search software should only be used if a small number of very specific documents have been requested, and it is not known which department or college holds them.

13. Format in which the personal data is to be provided.

Navitas will provide the information requested in a permanent form. This will usually be either a printout, photocopy, disc, or access for a period to electronic documents for downloading. If the request is made electronically, we should provide the information in a commonly used electronic format, if the customer is happy with this.

Where we have used codes within data, we will explain these to the requestor so that the documents will make sense.

14. Third party data

Individual rights do not automatically come with a right to personal information about anyone else (third parties).

The Divisional Privacy Manager is responsible for assessing the request, and removing third party data as required. Advice can be obtained from the Global Team if required. If any third party data is removed/redacted, this must be made clear in the response letter.

15. Requests for large amounts of personal data

Where we process a large quantity of information about an individual, the legislation permits us to ask the individual to specify the information the request relates to.

There is no exemption for requests that relate to large amounts of data, but such requests could be considered manifestly unfounded or excessive (as explained above).

Decisions on whether a request is manifestly unfounded or excessive should be agreed with the Global Team. There is a heavy onus on releasing information by Regulators, so having the Global Team agree will add required evidence to the decision.

16. Exemptions and restrictions

In some circumstances we might have a legitimate reason for not complying with a subject access request, so legislation provides several exemptions from the duty to do so.

This might mean that we refuse to provide all or some of the information requested.

UK exemptions are as follows:

- Legal Professional Privilege
- Self-Incrimination
- Corporate Finance
- Management Forecasts
- Negotiations
- Confidential References
- Exam Scripts and Exam Marks

Note, these exemptions also apply to the Right to be Informed. Divisional Privacy Managers, with the assistance of the Global Privacy Team, are responsible for applying them as and when appropriate to do so. Applying the right exemption requires data protection experience, and so should not be attempted by any employee outside of the privacy teams.

Any exemptions applied need to be disclosed to the requester via the response cover letter, including where any redaction of 3rd party personal data has taken place.

17. Refusing a request

Where requests are manifestly unfounded or excessive, as described above, rather than charge a

fee, if we prefer, we can refuse to respond.

Where we refuse to respond to a request, we must:

- Explain to the individual why we will not respond to their request.
- Do so without undue delay and at the latest within one month.
- Inform them of their right to complain to the ICO and to a judicial remedy once the ICO has issued their report.

Decisions on whether a request is unfounded or excessive will be done by the Global Team, to ensure that all angles and considerations have been made. Requests should be approached with a view to taking all steps to support the requester.

18. Responses

All responses to requests, either those agreeing with the requester, or those disagreeing, must be sent before the one month deadline period. A full explanation, including any relevant exemptions, will be included. The response will also include the right to an appeal or make a complaint to the Regulator.

19. Logging and filing requests.

All Data Subject Rights are to be logged on to the central register. This information will be used for reporting, root cause analysis and as evidence of the full request and response, should a Regulator request a copy.

Folders in the DSR SharePoint site are created per new request and all correspondence concerning the request is to be saved here. File naming is year – month – date – requester surname – Ref number – file type.

File naming examples

2023 06 02 Smith 001 Acknowledgement

2023 06 02 Smith 001 Response

The data subject rights log is the responsibility of the central team. Management of the requests within the log, to ensure they are up to date, accurate and in the correct status is the responsibility of the Divisional Privacy Manager who responds to the request.

20. Template letters

Any official response to a request should be made using the template letters which are available in the SharePoint folder.

Responses to Right of Access requests must also contain the following (as described in Article 15 of the EU GDPR).

- 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, in particular recipients in third countries or international organisations
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- the existence of the right to request from the controller 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 a supervisory authority
- where the personal data are not collected from the data subject, any available information as to their source
- the existence of automated decision-making, including profiling, with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

21. Complaints/Appeals

Any complaints or appeals received because of a data subject rights response will be managed by the Global Privacy Team, since they need to be independent of the original response. Any appeals or complaints about a response is to be sent to the Global Team immediately.

22. Root Cause Analysis & Quality Assessments

The Global Privacy Team will conduct root cause analysis and quality assessment annually. The results from this will form part of the annual privacy review document, to be presented to ELT.

Root cause analysis will investigate the reasons for the data subject rights requests and reveal any trends or re-occurring patterns.

Quality assessment will be conducted on random requests, to determine the appropriate measures and steps are being taken in line with this procedure and data protection legislation.

Looking at their request file and making sure file naming, correct templates, and the responses are all correct.

23. Offences

The UK Data Protection Act 2018 has a small number of offences listed. Two of these offences are related to data Subject Rights.

1. Section 173 - Alteration etc of personal data to prevent disclosure to data subject.

In the event of a Right of Access Request, it is an offence to alter, remove, destroy etc documents to avoid having to release them to the requester.

This is a common occurrence to avoid a complaint, or negative publicity, or worse legal action.

Not only is it an offence under the Data Protection Act 2018, but it is also not acceptable to Navitas. If there are concerns over information to be released, the person in the department or college which holds the data is required to speak with the divisional privacy manager and explain their concerns. If the concerns are valid, and no exemption exists, then the issue will be escalated to the Head of Department or College Director/Principle to make them aware of the risks, when the information is released.

2. Section 184 - Prohibition of requirement to produce relevant records.

It is a criminal offence to require an individual to make a subject access request.

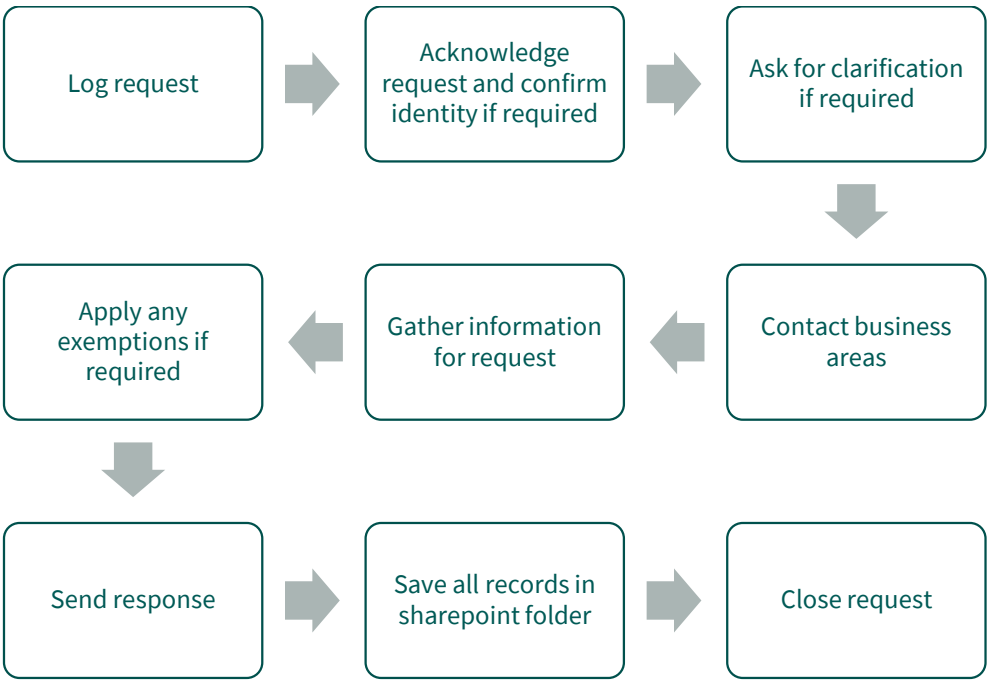
Navitas will not be requesting any individuals, students, employees, or partners, make a subject Access Request on our behalf because we wish to know information about.

If a suspected subject access request is being made in these circumstances, we will not comply with the request until we are satisfied the requester freely wants us to do so.

In many cases this type of forced request is in connection with employment, and in the past, it was common for a new employer to request a candidate to make a subject access request to the previous employer and hand over the information for review. This is now an offence, and Navitas will not participate in any way.

If any Navitas employee suspects that either of the above scenarios are taking place, the Global Head of Data Privacy & DPO should be informed immediately via email on kristie.marshman@navitas.com

24. Simple requests process map


Log request
Acknowledge request and confirm identity if required
Ask for clarification if required
Contact business areas
Gather information for request
Apply any exemptions if required
Send response
Save all records in sharepoint folder
Close request