Global Personal Data Sharing Policy

Navitas Group

Document

Document Name	Global Personal Data Sharing Policy
Brief description	This policy, which will be supported by a Data Sharing Procedure, sets Navitas' expectations when sharing personal data of individuals with external organisations. It provides instruction on how Navitas approaches its legal and regulatory obligations regarding the sharing of personal data. It points to the underpinning procedure that outlines Navitas' data sharing processes and requirements. It also sets out the requirements (and a template) for data sharing agreements which must be completed and agreed by the parties for all data sharing arrangements.
Responsibility	Global Head of Data Privacy
Initial Issue Date	12 March 2024

Version Control

Date	Version No.	Summary of Changes	Reviewer Name and Department/Office
2 Feb 2024	1	Initial version	Global Head of Data Privacy

Contents

1. Introduction

Sharing personal data with other organisations is often necessary. Privacy legislation allows sharing of personal data or individuals if it is lawful and meets privacy requirements. Information Sharing Agreements solidify those sharing arrangements, document the controls, and provide evidence and operational parameters.

This policy, which will be supported by a Data Sharing Procedure, sets the high level expectations when sharing personal data with external organisations.

2. Purpose

This policy provides instruction on how Navitas approaches its legal and regulatory obligations regarding the sharing of personal data. It points to the underpinning procedure which sets out Navitas' data sharing process and requirements, and requires that a data sharing agreement be completed and agreed by the parties prior to them sharing Personal Data. A template form of data sharing agreement that can be used for this purpose is annexed to this policy.

3. Scope

This Policy is effective across the Navitas Group and applies to all staff, contractors and consultants ("processors/users") of Personal Data, in addition to any requirements of local privacy laws.

This policy applies to all personal data no matter what medium it is collected and processed by. This will cover electronic records, paper records, DVDs, CDs, CCTV footage and any other type of medium which can hold personal data. USB or memory sticks are prohibited for use within the Navitas Group and should never be used to store personal data.

4. Definitions

Data controller - A data controller is an organisation which decides what personal data to collect, and how it will be used.

Data processor – A data processor does not decide what personal data to collect, nor how to use it, it only processes personal data under written instructions from the data controller.

Navitas or Navitas Group means Marron Group Holdings Pty Ltd ACN 631 941 403 (the ultimate parent company of the Navitas Group) and each of its subsidiaries. The term **Board** refers to the Board of Marron Group Holdings Pty Ltd.

Personal Data – any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Sharing Agreement – Document which records sharing parameters and documents privacy control and compliance measures.

Data Protection Impact Assessment (DPIA) – Personal data risk assessment, in some circumstances conducting a DPIA before sharing personal data is a legal obligation under the GDPR.

GDPR means the European Union's General Data Protection Regulation and the UK-retained version of that regulation.

Information Sharing – Sharing personal information between two data controllers, in a regular and agreed set of parameters.

Processing –Any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Supervisory Authority – Regulators for privacy in any country in which the Navitas Group operates.

Special Category Data - Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences or related proceedings, and genetic and biometric information.

5. Policy Requirements

5.1 When a sharing agreement is required.

A sharing agreement is put in place between two, or more, data controllers who wish to share personal data for legitimate purposes. Identifying when an organisation is a data controller is necessary in ascertaining whether a data sharing agreement is required.

The GDPR defines a data controller as:

> "An organisation which decides what personal data to collect, and how to use it."

A data sharing agreement is not required in the following scenarios.

- Between Navitas and suppliers/vendors – this is generally a relationship where Navitas is the data controller and the supplier/vendor is the data processor. In this case, privacy and data protection matters would be covered in the contract with the supplier/vendor or in a separate data processing agreement.
- "Internal" personal data sharing within the Navitas Group – this is covered by the Intra-Group Data Sharing Agreement which Navitas Group entities that are subject to the GDPR have entered into.

5.2 What does your sharing agreement need to achieve?

A data sharing agreement achieves three main purposes, as listed below.

- Privacy legislation – documents legal requirements
- Privacy regulators – provides documented evidence should it be requested for scrutiny.
- Operational staff – documents sharing parameters.

An information sharing agreement contains details of privacy legislation requirements and how those will be met or satisfied to ensure sharing is lawful. It also meets the accountability requirements under Principle 7 of the GDPR.

Should there be any complaints to a privacy regulator, the data sharing agreement will also contain the information that would be requested as part of their complaint investigation.

The information sharing agreement will contain operational requirements to ensure the data sharing remains consistent and compliant with agreed parameters. Navitas employees who will be managing the data sharing will be expected to use the data sharing agreement to ensure agreed instructions and requirements are followed appropriately, especially documented security requirements to keep the personal data secure.

Any advice needed on information security can be sought from the Global Head of Information Security gavin.ryan@navitas.com

5.3 What must be included in a sharing agreement.

A data sharing agreement needs to contain the appropriate compliance information. It must outline exactly what personal data is being shared, and why. To achieve this, the following headings are present in the sharing template, and must be completed.

- Who the parties are to the agreement.
- What the purpose of the sharing is
- The aims, necessity, and benefits
- The organisations that will be involved in the data sharing.
- Is the sharing two ways with another organisation?
- A list of data sets to be shared.
- The lawful basis for sharing
- A list of any special category data, sensitive data, or criminal offence data to be shared.
- The process for managing data subject rights requests, and other legal access rights.
- The information governance arrangements in place

5.4 What further details should we include?

- How the privacy principles will be met
- How the information will be shared securely
- Who is operationally responsible for the sharing for each organisation?
- Annual monitoring form

5.5 Sharing agreement process

Data sharing agreements are privacy specific documents, as such they need to be drafted by a privacy expert.

Should a department or college have a requirement for an information sharing agreement, they are to contact their Divisional Privacy Manager.

There will be circumstances where a Data Protection Impact Assessment (DPIA) may need to be done beforehand, which the Privacy Manager will confirm. The Data Sharing Procedure explains this process in more detail.

5.6 Sharing in an emergency.

If there is a serious risk of harm to human life, then sharing data should be deemed necessary.

Information needing to be shared in these situations should always be the minimum amount of personal data, and the personal data must be shared securely. A member of the privacy team should be consulted in these instances either before the information is shared (only where reasonably practicable) or as soon as practicable thereafter.

Good examples of what can be deemed an emergency are included guidance provided by the Information Commissioners Office (ICO), the UK Privacy Regulator and include:

- Preventing serious physical harm to a person
- Preventing loss of human life
- Protection of public health
- Safeguarding vulnerable adults or children
- Responding to an emergency
- An immediate need to protect national security.

6. Roles & Responsibilities

6.1 Executive Leadership Team

- Promulgating and promoting this policy
- Approving any changes arising from the annual review of this policy if any changes are

recommended.
- Supporting the requirement for data sharing agreements as required by this policy

6.2 Data Protection Officer (UPE)

Note: The Global Head of Data Privacy is also the Data Protection Officer for UPE

- Provide advice on data sharing and data sharing agreements.
- Provide advice DPIA's where they are required for data sharing purposes.
- Serve as the main point of contact for Supervisory Authorities for data protection and privacy.

6.3 Global Head of Data Privacy (GHDP)

- Provide advice on data sharing and data sharing agreements.
- Provide advice DPIA's where they are required for data sharing purposes.
- Support senior management and global data sharing agreements.
- Accountable for data sharing agreement process
- Own and review data sharing policy.

6.4 Divisional Privacy Managers

- Be operationally responsibility for the data sharing agreement process
- Draft data sharing agreements for approval by GHDP (where required)
- Complete DPIA for the data sharing where appropriate
- Review divisional data sharing procedures to support this policy
- Annual review of data sharing agreements using monitoring form.

6.5 Heads of Departments and Business Units

- Promote this policy, and associated procedures to their teams.
- Ask the Privacy Team for guidance as and when required.
- Notify their divisional Privacy Manager when a data sharing agreement may be required.

6.6 Navitas employees and third parties who have access to Navitas personal data

- Adhere to this policy and associated procedures.
- Identify when a data sharing agreement is required and engage with their Divisional Privacy Managers to have them prepared.
- Follow operational parameters in the data sharing agreement once signed and in progress.
- Seek advice and guidance from divisional Privacy Managers where needed

7 Enforcement

All Navitas employees are responsible for complying with this Policy and applicable laws, rules, and Regulations. Known or suspected violations of this Policy must be immediately reported to a supervisor or manager, and the Global Head of Data Privacy.

Any individual who violates this Policy may be subject to disciplinary action, which, depending on the nature of the violation and the history of the employee, may range from a warning or reprimand to, and including, termination of employment.

8 Changes to this Policy

This policy is to be reviewed annually, considering changes to legal, regulatory, or contractual requirements, changes in working practice or structure of the business. Changes to the policy may also be as a direct result of inputs from audits, security incidents, risk assessments, improvement actions and new objectives.

Any suggestions on how to improve the policy can be sent to the Privacy Team at privacy@navitas.com

Navitas Data Sharing Agreement

Between

****

And

****

1. Party details

Organisation	Name	Address	Primary contact
Party 1			
Party 2			

2. Commitments

The Parties recognise the importance of complying with their obligations under applicable data protection laws when they share personal data in the context of their relationship. Each party shall assist and co-operate with each other to enable each other to comply with applicable data protection laws to which they are subject.

Each party commits to only use and keep personal data received from the other party in accordance with the purposes and requirements set out in this data sharing agreement. Each party shall ensure personal data is kept confidential and secure and will not disclose or allow access to personal data provided by the other Party except as contemplated by this data sharing agreement; and appropriate technical and organizational measures are in place to protect against unauthorized or unlawful access or use of personal data and against loss or destruction of personal data.

3. What is the purpose of the sharing?

Describe each of the below to support the data sharing.

- the specific aims of the sharing
- why the data sharing is necessary to achieve those aims
- the benefits to the individuals and the business

Specific aims of sharing	
Why data sharing is necessary to achieve those aims.	
Benefits to the individuals and the sharing parties	

4. What are the personal data/data sets to be shared?

Organisation	Data Sets	Lawful basis	Shared with
Party 1			
Party 2			

5. Will you share special category data or criminal offence data?

Special category data will require an article 9 condition to be identified, and in some instances, depending on which Article 9 condition is used, also a Schedule 1 condition from the Data Protection Act 2018.

Other global legislation may differ, privacy managers will be required to check local requirements dependent on parties involved and legal regimes engaged.

NO / YES*
* If yes, provide details:

6. How will you meet the requirements of the GDPR Principles?

Principles	Sharing Party 1 ***	Sharing Party 2 ***
Principle 1 Fairness		
Principle 1 Lawfulness		
Principle 1 Transparency		

Principles	Sharing Party 1 ***	Sharing Party 2 ***
Principle 2 **Purpose Limitation**		
Principle 3 **Data Minimisation**		
Principle 4 **Accuracy**		
Principle 5 **Storage limitation**		
Principle 6 Security **Information Governance Arrangements**		
Principle 7 **Accountability**		

7. What will be the process for managing access rights?

All parties to this agreement will have in place the appropriate policies, procedures and training to facilitate requests under data protection legislation, and in the event of a public sector organisation, FOI and EIR.

Data subjects are allowed to make a request to either or both/all parties to this data sharing agreement,

- Data Subject Rights
- Freedom of Information
  Environmental Information Regulations

8. What information governance arrangements are in place?

Details of each party's information governance arrangements are to be detailed here.

Sharing Party 1 - Navitas	Sharing Party 2 ***
Ensure data sharing agreement is shared with team responsible for sharing. Ensure staff are trained in minimum online GDPR training. Under data subject rights requests and how to action Understand how to use the monitoring form and check data sharing is relevant and needed Understand the process of stopping sharing at the end of the initiative	

9. How will you share the personal information securely?

Enter details here of what method will be used to transfer the personal data being shared, and what controls will be in place to ensure this sharing is secure.

- Transfer method
- Organisational measures in place
- Technical measures in place

	Sharing Party 1 ***	Sharing Party 2 ***
Item 1 **Transfer method**		
Item 2 **Organisational measures in place**		
Principle 1 **Technical measures in place**		

10. How often will you share personal information?

This may depend on the method of sharing. For example, if you are sharing using email or file share this maybe monthly or weekly. However, if you are using a shared system with appropriate access controls, this will likely be constant sharing.

Sharing Party 1 ***	Sharing Party 2 ***

11. Who is operationally responsible for the sharing?

The individual/s who are operationally responsible are those who are managing the data sharing within each organisation. This is not the same person/people who are required to sign the data sharing agreement or contract.

This responsibility includes ensuring the parameters of this data sharing agreement are kept to, and carrying out annual monitoring using the template in Appendix B.

Sharing Party 1 ***	Sharing Party 2 ***

12. International Transfers

There are safeguards for transferring personal data globally. The Privacy Manager is responsible for scoping the transfers, the control requirements and then documenting the safeguards employed, depending on the legal regimes in place.

13. Data Breaches and Incidents

Whilst each party is a data controller, for the purposes of this sharing agreement, any serious or reportable data breaches should be notified to all party's signed up to the agreement.

The data controller responsible for the data breach has a legal obligation to determine the risks to the rights and freedoms of the data subject involved in the data breach, and it is there decision on whether the data breach is reportable or not. However, all data breaches involving parties to a data sharing agreement must be notified, so any legislative requirements placed on them are reviewed accordingly.

The individuals accountable for privacy in each organisation are to be detailed below, along with contact details.

Organisation	Name	Contact details
Navitas	Kristie Marshman – Global Head of Data Privacy	privacy@navitas.com
Party 2		

14. Communications with supervisory authorities

Parties to a data sharing agreement shall immediately notify the other Party/s and all shall use best efforts to assist each other in the event of any audits, enquiries, investigations, requests, orders or other proceedings or matters relating to this agreement by a supervisory authority or any other public body.

To the extent permitted under applicable law, parties shall use best efforts to assist each other and to ensure an aligned and coordinated communication with supervisory authorities.

In the event of a dispute with, orders or fines imposed, or other claims brought by a supervisory authority or other competent authority concerning the processing of shared data against either or both the parties shall promptly notify and inform each other. Parties shall cooperate and coordinate with a view to effectively defend themselves against such claims or settling them amicably in a timely fashion.

15. Intellectual property

Save where expressly provided for, in relation to ownership and licence of any intellectual property rights the Parties acknowledge and agree that the Party disclosing personal data to the other shall retain ownership of its personal data. With effect from such time as the a Party provides the other Party with its personal data, the disclosing Party grants a fully paid and royalty-free, worldwide, non-exclusive, transferable licence to the receiving Party to use any intellectual property rights in and to such personal data (to the extent the disclosing Party has the right to grant such a licence) for the purposes of and in accordance with, and subject to, the terms of this Agreement, and any instructions as notified by the disclosing Party from time to time.

16. Term and termination

This Agreement shall continue in full force and effect while ever there is any transfer of personal data between the Parties for the purposes described in this agreement and shall expire when the relationship between the Parties necessitating that purpose ends or a Party gives notice of termination of this Agreement.
Any termination of this agreement shall be without prejudice to any other rights or remedies of a Party under this agreement or at law and will not affect any accrued rights or liabilities of a Party at the date of termination nor shall termination affect any rights or obligations of the Parties which are to be observed or performed after such termination.

In the event of termination of this Agreement, each Party shall: (a) promptly return or permanently and securely delete the other Party's personal data, together with all copies in any form and in any media in that Party's power, possession, or control. Each Party's right to use the other Party's personal data obtained under this Agreement shall cease immediately on termination.

17. Governing law

This Agreement and any dispute or claim arising out of or in connection with it or its subject matter, existence, negotiation, validity, termination or enforceability (including non-contractual disputes or claims) shall be governed by and construed in accordance with English Law.

Signed by the duly authorised representative of each Party.

_____ Name & post:

On behalf of XXXX Organisation Date and email:

Name & post:

Date and email:

_____

On behalf of XXXX Organisation

Appendix B - Annual Monitoring Form

This form should be completed annually to ensure all parties to a data sharing agreement are still sharing lawfully and within the parameters set by the agreement. The originating data controller is responsible for ensuring this monitoring form is completed annually.

Is the purpose of the sharing still the same?	Yes/No (delete as appropriate)
Is the sharing only being used for the documented purpose/s?	Yes/No
Is the lawful basis for processing and sharing still the same?	Yes/No
Are the data sets still the same?	Yes/No
Could fewer personal data be shared to meet the identified purpose/s?	Yes/No
Have data controller responsibilities changed?	Yes/No
Have retention periods changed?	Yes/No
Are technical and organisational security controls still appropriate?	Yes/No
Has there been any information security incidents or data breaches?	Yes/No

Once the above is complete, each organisation is required to sign the below and keep a copy of this monitoring form.

On behalf of XXXX Organisation

Name & post:

Date and email:

On behalf of XXXX Organisation

Name & post:

Date and email: