Global GDPR & Privacy Policy

Navitas Group

Document Name	Global GDPR & Privacy Policy
Brief description	This document sets out Navitas' policy regarding the collection and processing of personal data. It outlines the requirements under the EU GDPR, which Navitas has adopted as its global standard as well as acknowledging additional requirements of locally applicable privacy legislation that may apply.
Responsibility	Global Head of Data Privacy
Initial Issue Date	June 2023

Contents

1. Introduction

Navitas is committed to protecting the rights and freedoms of living individuals by ensuring it lawfully and securely processes personal data in accordance with global data protection and privacy laws.

Navitas has adopted the EU GDPR (which is mirrored in the UK GDPR) across its global business, supplemented or adapted where required or appropriate to meet local legislative and regulatory requirements. This means that the EU GDPR generally applies to the collection and processing of personal data, no matter where in the world Navitas or the relevant individual is located.

Below are some of the other privacy laws which apply to Navitas in certain jurisdictions either due to location or due to the international students who attend our colleges. However, this is a not an exhaustive list and privacy laws are frequently being developed and updated.

Navitas businesses and employees are responsible for ensuring they conduct themselves in accordance with all applicable privacy laws. Navitas' privacy team will assist and support Navitas businesses and employees in this endeavour.

- Australia — Privacy Act 1988 (Cth)
- Canada — Personal Information Protection and Electronic Documents Act (PIPEDA)
- China — Personal Information Protection Law
- Singapore — Personal Data Protection Act of 2012
- UAE — Federal Degree-Law No. 45 of 2021 on the Protection of Personal Data

This policy governs how Navitas will collect and process personal data in accordance with the EU GDPR. Other privacy laws must be adhered to where applicable, but such requirements will be addressed in local policy and procedure, not in this overarching policy.

2. Purpose

This policy sets out how Navitas approaches its legal and regulatory obligations with regards to data protection. The GDPR is a wide and complex piece of legislation, and this policy and its supporting procedures are in place to ensure legal obligations are met and personal data is processed safely and securely. It will outline how employees, including contractors and consultants etc, must collect and use personal data within global legislative requirements.

3. Scope

This policy applies to all Navitas businesses and employees globally. It also applies to those who work on our behalf such as suppliers, consultants, or contractors who might be processing personal data for which Navitas is legally responsible for, as a Data Controller.

This policy applies to all personal data used by Navitas, no matter in which country it is collected and processed.

4. Definitions

Adequacy – The ICO or European Commission has deemed a country provides adequate levels of protection towards personal data, and transfers can take place without additional safeguards, allowing free movement of personal data.

Anonymisation – A process to completely remove any personal data from a dataset.

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

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.

Data Protection Impact Assessment (DPIA) – Risk assessment specifically for processing of personal data.

EU GDPR means the European Union (EU)'s General Data Protection Regulation, also known as Regulation (EU) 2016/679, as amended from time to time.

Exemptions – Identified parts of privacy legislation which allows processing outside of the legal requirement, in specific circumstances.

Information Commissioners Office (ICO) – The UK Regulator for GDPR and Data Protection.

Personal data - Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular 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.

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.

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.

Pseudonymisation – A process to replace personal identifiers, such as a name, address, ID, with an artificial identifier, such as a code or number.

Record of Processing Activities (RoPA) – A RoPA is a personal data asset register. A record of an organisations processing activities involving personal data.

Safeguards Policy – A legally required policy if processing special category data under certain circumstances.

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 —any use of special categories of personal data should be strictly controlled in accordance with this policy.

Supervisory Authorities – Regulators for GDPR across Europe and the EEA.

5. Policy Requirements

5.1 Data Protection Principles

The data protection Principles under the GDPR are a set of requirements on how personal data must be collected and processed. All Navitas employees must be familiar with these Principles and apply them to the collection and processing of personal data. The Principles below apply to all processing of personal data, including existing and newly collected data.

1(a) Lawful, fair, and transparent

Lawful

Navitas will not break any other law in the collection and use of personal data, and it will identify a correct lawful basis to use that personal data. The lawful bases are set out in Article 6 of the GDPR, and the Privacy Team are responsible for identifying and recording the correct basis.

Fair

Navitas will ensure that at a fundamental level, the collection and use of personal data is “fair”. The individuals whose data is being collected will have a “reasonable expectation” their data will be used in this manner. Navitas will not use personal data in a manner that is detrimental to the individuals, nor will it mislead them about how their personal data is to be used.

Transparent

Transparency is a vital component of privacy. Navitas will ensure that where personal data is collected and used, that it is transparent. Navitas will achieve this by providing a privacy notice at the point personal data is collected.

Prior to collecting new personal data in a new way, or processing existing data for new purposes, advice should be sought from the Privacy Team.

1(b) Purpose Limitation

Personal data will be collected for one or more specific purposes. It must not then be used for something which is incompatible with the original purpose(s).

Navitas will clearly communicate at the point personal data is collected, via privacy notices, the purpose(s) for which the personal data is being collected. These purposes will also be documented in the Navitas RoPA.

Navitas employees are required to ensure that personal data is used for the original purpose(s) only, and that any changes to proposed use are discussed with the Privacy Team before any changes in processing begin. If changes to the purpose of personal data are required, and these are different to the original purpose then the following is required:

- A compatibility test is completed by divisional privacy managers, and if compatibility is confirmed the new processing can take place once documentation has been updated, including privacy notices.
- If compatibility is not confirmed, then processing under the new purpose can only take place with the prior consent of the individuals involved.

1(c) Data Minimisation

The GDPR requires the use and storage of personal data to be adequate, relevant, and limited to what is necessary, for the identified purpose to which it was collected and processed.

Navitas employees are responsible for only using the required amount of personal data for any given purpose. Sense checking the personal data, to ensure it is adequate, relevant, and limited to what is required, is the responsibility of all. The Privacy Team can be called upon for advice whenever needed.

1 (d) Data accuracy

Personal data collected by Navitas must be accurate, and where necessary, kept up to date. This is achieved by taking all reasonable steps to ensure the personal data is accurate at the point of collection, and any inaccuracies corrected as they are identified, where required.

Navitas employees are responsible for ensuring all reasonable endeavours be made to keep personal data up to date and accurate.

1(e) Data limitation

Personal data must not be kept longer than is necessary. Navitas will develop retention schedules which will be set out in the Records Management Procedure. The retention schedule will detail how long personal data is to be kept for and will be reviewed annually.

Employees are responsible for using the retention schedule to ensure personal data is not kept longer than required.

1(f) Integrity & confidentiality

Navitas is committed to keeping all personal data safe and secure. The appropriate technical and organisational measures are in place to ensure the integrity, confidentiality, and availability of personal data.

Employees are responsible for keeping the personal data that they use safe and secure. They are responsible for understanding the organisational and technical measures in place to protect the personal data they use. These measures include actions which are proactive on the employees' part, such as attending available training when offered, and engaging with the Privacy Team and Information Security Team.

2(a) Accountability

This Principle requires Navitas to document and evidence all measures taken to meet GDPR accountability obligations. Navitas will document the technical and organisational measures implemented to keep personal data safe, as well as the other controls it uses to meet areas of compliance as required.

Types of controls Navitas can demonstrate accountability under are Privacy Notices, Policies, DPIA's, appointing a DPO, issuing training and awareness, and the Navitas Record of Processing Activities (RoPA). However, this is not an exhaustive list.

The Privacy Team will support Navitas businesses and employees by assisting in identifying, implementing, and documenting compliance controls.

5.2 Incident management & data breach investigations

Navitas is committed to investigating all information security incidents and data breaches and has a robust incident management process.

If an employee discovers a data breach, they are required to report it immediately through approved channels and follow instruction by the Privacy Team to assist with the resulting investigation.

The Data Breach Procedure provides details on how that process works, and which internal stakeholders are involved. It also provides structure and process maps, along with responsibilities to ensure data breaches are managed consistently.

Navitas has incident and data breach training in place. Employees are expected to attend the training when offered, to enable them to recognise data breaches and required to report them through approved channels.

5.3 Data Subject Rights

There are 8 Data Subject Rights documented in the GDPR. They are listed below.

- Right to be Informed
- Right of Access
- Right of Rectification
- Right of Erasure
- Right to Restriction of Processing
- Right to Data Portability
- Right to Object
- Right not to be subject to Automated decision-making, including Profiling.

Any individual whose data Navitas collects and uses, is entitled to exercise one or more of the above “Rights.”

All Navitas employees are responsible for recognising the above rights and reporting breaches of those rights through the correct channels to the Privacy Team. All employees can contact the Privacy Team via privacy@navitas.com

Individuals can send their Data Subject Rights request to any part of Navitas, and it is at this initial date (barring any ID required) that the 1-month legal deadline to respond begins. It is vital that employees therefore recognise a request, and send it to the Privacy Team. This must be done within 24 hours (less where possible) of receiving the request.

All requests will be logged and managed by the Privacy Team.

5.4 Special category data

Special category data is personal data that the GDPR has given extra protection because of its sensitive nature.

Special category data is listed below.

- personal data revealing **racial or ethnic origin**.
- personal data revealing **political opinions**.
- personal data revealing **religious or philosophical beliefs**.
- personal data revealing **trade union membership**.
- **genetic data**.
- **biometric data** (where used for identification purposes).
- data concerning **health**.
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Navitas will document the collection and use of special category data in the RoPA (Record of Processing Activities) and the technical and organisational measures in place to protect it.

If any employee of Navitas wishes to collect or use any personal data falling into the above special categories of data, they must contact the Privacy Team first who will identify whether a Data Protection Impact Assessment needs to be completed before any personal data is collected. When processing special category data, a lawful condition under Article 6, and under Article 9, will need to be identified. If there is not a lawful condition for processing available, then any collection and use of special category data is prohibited under the GDPR and Navitas will not approve the collection and use of that special category data.

5.5 Data Protection by Design and by Default

Navitas applies a data protection by design and by default approach to the collection and processing of personal data. This means that data protection and privacy requirements must be considered as part of everything Navitas does from inception. Examples of where Navitas will apply data protection by design and default include at the beginning of projects, when choosing suppliers, and when implementing the appropriate levels of technical and organisational measures to protect personal data.

Further details of Navitas' data protection by design and by default can be found in supporting Procedures.

5.6 Records of Processing Activities (RoPA)

The GDPR requires Navitas to keep a Record of Processing Activities (RoPA). Navitas has a RoPA, and it is updated annually by the Privacy Team.

The GDPR provides specific details of what needs to be recorded in a RoPA, this includes items such as the purpose of the personal data, the types of personal data, who it will be shared with and retention periods.

All employees who are contacted by the Privacy Team and asked to update the RoPA for their area, are required to do so within the timeframe provided by the Privacy Team. The advised timeframe will not be less than two weeks, to ensure employees are not disrupted by annual leave or work deadlines, etc.

5.7 Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessments (DPIAs) are a privacy risk assessment tool to determine the risks to individuals when an organisation is collecting and processing personal data.

Navitas will complete DPIA's where they are a legal requirement, and in circumstances where they are considered good practice. Navitas has adopted the UK ICO guidance for identifying when a DPIA is good practice, using the ICO's screening questions.

Further guidance regarding DPIA's can be found in the DPIA Procedures document. Additionally advice can be sought from the Privacy Team.

5.8 Anonymisation & Pseudonymisation

Anonymisation

Truly anonymised data, with all identifiers of an individual removed, is not considered personal data by the GDPR.

The GDPR places an obligation on organisations to anonymise personal data if it is no longer needed to identify individuals. As such Navitas requires all employees to ensure any personal data is anonymised if appropriate to do so. Where personal data is required to be held, no anonymisation needs to take place. Anonymisation is often useful if statistical information is required, but not the personal data itself.

Pseudonymisation

Pseudonymisation is a process in which certain personal data identifiers, such as a name, address, or ID etc, are replaced, for example with a code, or a number. Privacy legislation requires that the process of pseudonymisation is carried where appropriate to reduce the risks to individuals.

Advice must be sought from the Privacy Team should employees have reason to believe they should anonymise or pseudonymise personal data.

5.10 Data Processors

The term Data Processor is used to describe suppliers and/or vendors who supply goods or services directly to Navitas, its partners, and universities, and processes personal data on our behalf. Where Navitas uses a supplier/vendor in a data processor capacity it will carry reasonable due diligence before engaging with them.

Navitas employees should notify their Divisional Privacy Team of new suppliers and/or vendors.

The relevant Privacy Team will assist Navitas businesses ensure that the required contractual clauses are present in contracts in place with Navitas suppliers and vendors to ensure Article 28 (3) is satisfied.

Navitas has a Procurement Policy and Vendor Access Policy which provides guidance and support to ensure suppliers are protecting the personal data processed on our behalf.

5.11 International transfers

There will be circumstances where it is necessary for Navitas to transfer personal data internationally. Where this happens Navitas will ensure the transfer of personal data is lawful. Depending on the purpose of the transfer and where the personal data is transferred to, will determine which legal safeguards need to be in place.

Guidance and support to fulfil legal obligations around transferring personal data internationally is to be sought from the Privacy Team.

Internal data sharing, due to Navitas being a global organisation, is essential to business objectives. To ensure that transfers of personal data between Navitas businesses are secure and lawful, the relevant Navitas Group members have entered into a Intra Group Data Sharing Agreement that governs the rights and obligations in relation to personal data transferred between them.

5.12 Audits and Monitoring

Data Protection audits and monitoring are conducted to assist with mitigating privacy risk, and to meet GDPR Article 39 requirements. Compliance monitoring and audits will be supported by relevant procedure documents, and any monitoring which involves employees will be transparent and included on relevant employee privacy notices.

External audits, as required under contract clauses with suppliers as part of Article 28 obligations, will be documented in data processing agreements.

Data Protection audits will be carried out by the Privacy Team.

5.13 Training and Awareness Program

Navitas will create and keep up to date a Training and Awareness Program. This program will cover the following areas.

- Mandatory online training in data protection and information security for new starters
- Mandatory refresher training for all staff annually
- Training for external parties with access to Navitas personal data, such as consultants
- Bespoke training for high risk areas such as HR, Health & Safety and Marketing
- Ongoing awareness campaigns
- Bespoke topics such as data breach training and data subject rights training

All training will include assessment and feedback to ensure value and accountability.

Training and Awareness Program will have senior management sign off and be reviewed yearly against training analysis incorporating risk management and reporting results.

6 Roles & Responsibilities

6.1 Navitas Board

- Overall responsibility for management of the Navitas Group, including oversight of data protection & information governance

6.2 Executive Leadership Team

- Agreeing and approving the content of this policy
- Promulgating and promoting this policy
- Approving the annual review of this policy
- Ensuring the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data
- Supports the Data Protection Officer in the performance of their tasks
- Ensure the Data Protection Officer does not receive any instructions on how to perform those tasks

6.3 Data Protection Officer

- Serve as the main point of contact for Supervisory Authorities/Regulators for data protection and privacy
- Cooperate with Supervisory Authorities/Regulators
- Monitor compliance with applicable privacy legislation, including awareness raising and training, audits, and assignment of tasks
- Provide advice where required on DPIA's and any other risk assessment involved privacy and data protection

6.4 Global Head of Data Privacy

- Heads the global privacy function at Navitas
- Accountable for implementing and maintaining privacy excellence across the business
- Responsible for providing accountability and reporting to senior management to ensure visibility of privacy landscape.
- Continuously report on progress and maintenance of privacy risks
- Lead the Privacy Team to ensure the best possible privacy compliance across the business
- Ensure value for money on automation tools and resource

6.5 Data Privacy Managers

- Responsible for managing the processes and obligations in this policy
- To provide advice and guidance proactively when requested on the subjects in this policy

6.6 Heads of Businesses 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

6.7 Navitas employees and 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
- Applying the Data Protection Principles to all processing of personal data
- Responsible for keeping personal data safe and secure
- Responsible for not losing or misusing personal data

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 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.