Data Protection Policy

1. Summary & Purpose

The purpose of this document is to demonstrate the Management Board's commitment to the protection of personal data.

Signify processes personal information on a daily basis as part of its business operations. The processing of personal information occurs mainly for use in the client Signify System.

It is important that Signify's Directors, employees and third parties adopt responsible data privacy practices. This entails adhering to applicable data protection/privacy legislative and regulatory requirements, demonstrating good corporate governance, safeguarding the integrity of personal information that Signify processes, and maintaining a good reputation.

We are committed to preserving the confidentiality, integrity, and availability of all the physical and electronic information and information-related assets relevant to meeting the purpose and goals of the organisation. This includes the handling of personal data or "personally identifiable information" (PII).

The purpose of this Data Protection Policy is to ensure that:

- the privacy rights of clients are protected;
- personal information processed in Signify is protected;
- Signify complies with all applicable regulatory and statutory requirements;
- Signify fulfils all its responsibilities for relevant data protection and other regulatory authorities, where applicable, to conduct business in an ethical, open and transparent manner; and
- third parties comply with the privacy principles as contained in this Data Protection Policy.

2. Policy Statement

1. All information must be handled in accordance with the following documents:
    - Terms & Conditions of Employment (*control 6.2*)
    - Acceptable Use of Assets Policy (*POL 08_ Signify IT Acceptable Use Policy*)
    - Code of Conduct (*POL 07_ Signify Code of Conduct*)
2. Information must also be handled in accordance with the table below.
3. Where customer information must be handled in line with their requirements and/or classification scheme, those requirements will take precedence (e.g. for the government etc.).

Level	Handling
"Public"	1. The organisation has structured and approved the information prior to release and is satisfied for it to be transmitted to unknown persons. 2. Removable media may be used to store or transfer this information, but it is strongly recommended that the media be erased once the task has been completed.

"Confidential"	1. Hard copies are acceptable but this is deemed **"uncontrolled"** and must be kept within the confines of the office as best practice.
	2. Personnel can take hard copy information outside of the premises if there is a clear business reason to do so but must return it for storage or secure destruction when finished.
	3. Information can be passed on to third parties where:
	  1. suitable NDAs are in place;
	  2. sufficient checks are made for the suitability of sending; and
	  3. the information owner has granted the appropriate permissions.
	4. Information may be stored or transferred using removable media provided that:
	  1. the media is encrypted; and
	  2. appropriate permissions are granted from the information owner.

"Sensitive"	1. This information may be transferred only between authorised persons.
	2. The printing of information must be avoided where possible.
	3. Where printing is unavoidable, information must be recovered from the printer immediately.
	4. Hard copies must not be taken off-site unless express permission has been granted by the information owner.
	5. Hard copies must be stored in designated storage facilities (e.g. locked filing cabinets).
	6. Information may be stored or transferred using removable media, provided that:
	  1. the media is encrypted; and
	  2. appropriate permissions are granted by the information owner.
	7. The storage or transfer of personally identifiable information (PII) using removable media must be avoided wherever possible. Where the use of removable media is required, advice must be sought from the Data Protection Officer to ensure compliance with legislation.

4. Scope and Applicability

This Data Protection Policy applies to the processing of all records of personal information and applies to the following:

- All Directors and employees
- All personal information under the possession, control and/or ownership of Signify, whether located at Signify or non-Signify locations, and in all formats including electronic or physical formats
- Any device or IT infrastructure used to process personal information in Signify's information processing facilities, or which are authorised to access Signify's information processing facilities

This policy sets out the privacy and data protection principles which Signify as the data controller/responsible party is required to comply with, as well as third parties and data processors/operators.

The Directors and management team of Signify have ownership and oversight of this policy and the related procedures, and are responsible for ensuring compliance with this policy, as well as any local privacy and data protection legislation, regulations, rules and guidelines.

5. Input & Reference Documents

POPI Act sections 2 to 38; sections 55 to 109; sections 110 to 111; and section 114

ISO 27001:2022 standard, A.5.34 and A.7.7

6. Definitions

Data subject	"Data subject" means an individual who is the subject of personal data.
Personal data	"Personal data" is 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 one or more factors specific to the physical,

	physiological, genetic, mental, economic, cultural or social identity of that natural person.
Sensitive personal data	"Sensitive personal data" is any 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. Any use of sensitive personal data should be strictly controlled in accordance with this policy.
Controller	"Controller" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Processor	"Processor" means a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.
Recipient	"Recipient" means a natural or legal person, public authority, agency, or another body, to which the personal data is disclosed, whether a third party or not.
Processing	"Processing" means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, 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.
Profiling	"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, their economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Consent	"Consent" of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to them.
Personal data breach	"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

7. Key Privacy Principles

To effectively implement this policy, Signify must assign accountability for its data protection and privacy policies and procedures across Signify, as follows:

- Assigning a responsible person or persons to ensure the principles contained in this policy are affected and, where applicable, legislative, and regulatory requirements in their jurisdiction
- Defining, documenting, and communicating to Signify's Directors, employees and third parties all data privacy and data protection-related policies, notices, and procedures
- Being able to demonstrate the Company's compliance with this policy as well as the applicable regulatory requirements
- Defining, documenting and communicating a data protection operating model and clearly indicating all relevant roles and responsibilities that will give effect to the policy statements contained in this policy
- Implementing adequate training, awareness and cultural change initiatives to ensure that Signify's Directors and all employees are aware of and understand the data protection requirements as set out in this policy, as well as any privacy or data protection procedures implemented in Signify

8. Processing Limitations

Personal information must be processed lawfully and in a manner that does not infringe the privacy rights of a client. Personal information should be processed only when required to do so by Signify:

- Where the processing is adequate, relevant, and not excessive considering the purpose

- Where the processing of personal information is required so as to comply with statutory and/regulatory requirements
- Where the processing of personal information is required to carry out actions for the conclusion or performance of a contract to which the client is a party
- Where the processing of personal Information is required to protect the legitimate interests of the client
- Where the processing is required for pursuing the legitimate business interests of Signify (e.g. to carry out Signify's licensed or business operations) or of a third party to whom the personal information is supplied

9. Retention of Personal Information

Records of personal information must not be retained any longer than is necessary for achieving the intended purpose.

10. Security Safeguards (Including the Clear Desk and Screen Policy, and password policy)

Signify must protect and secure all personal information under its control by implementing technical and organisational measures and procedures. These measures and procedures include but are not limited to:

Signify's Clear Desk and Screen Policy, which states the following:

- Sensitive information must not be left alone or exposed to unauthorised users at any point.
- Confidential information on paper or electronic storage media must be secured when not required, especially when the office is vacated (ideally in paperless form in the first instance, otherwise locked in a desk pedestal, filing cabinet or other furniture in the office).
- Documents containing confidential or sensitive information must be removed immediately from printers.
- Devices must have a lock screen enabled.
- There is no need to physically secure devices if the room in which the device is held has adequate security (e.g. the door locks or it is located at a trusted premises).
- If there is any safety concern, employees must take their device with them.
- If users are working where unauthorised parties might have a view of their screen, they must do the following:
    - Move, so that the unauthorised parties do not have a view of their screen
    - Apply a privacy screen to the device

- Ensure that they are working on public information and no higher in classification

The password policy which is enforced by a pre-configured policy on the network. Which include the following:

1. **Minimum Password Length: 11**
   - Passwords must be at least 11 characters long.
2. **Password Complexity Enabled: True**
   - Passwords must include **at least 3 of these 4 types**:
     - Uppercase letters (A–Z)
     - Lowercase letters (a–z)
     - Numbers (0–9)
     - Special characters (e.g., !, $, #).
3. **Password History Count: 2**
   - Users cannot reuse their last 2 passwords.
4. **Maximum Password Age: 90 days**
   - Passwords must be changed every 90 days.
5. **Minimum Password Age: 7 days**
   - Users must keep a password for at least 7 days before changing it.

The Account lockout policy which is enforced by a pre-configured policy on the network. Which include the following:

1. **Lockout Threshold: 10**
   - Accounts lock after 10 failed login attempts.
2. **Lockout Duration: 15 minutes**
   - Locked accounts automatically unlock after 15 minutes.
3. **Observation Window: 15 minutes**
   - Failed login attempts are tracked over a rolling 15-minute period.

11. Information Backup

As an organisation that primarily uses cloud-based technologies, replication, and backups are the responsibility of cloud service providers.

Through the implementation of controls relating to the management of supplier relationships (*controls 5.19 - 5.22*), we gain assurance that backup and continuity requirements are met. Suppliers are selected based on several criteria for consideration, including data replication and backup.

For online services

Our cloud service providers are selected based on their ability to provide replicated-data architecture with the provision of built-in data backup and high availability (also refer to *MNMT-PROC-10_Signify Equipment Verification*).

For documentation and file storage

SharePoint Online is used to store internal documents. The service provisioned by Microsoft includes a high-availability, replicated, and backed-up environment.

12. Purpose of Collecting Personal Information

Signify collects personal information of client's employees to be imported into the Signify System as part of our support and implementation services, allowing other information relating to the system to be linked to the personal information. This includes but is not limited to:

- People Management
- Performance Management Data
- Personal Development Plan Data
- 360 Employee Evaluation Data
- Job Profiling
- Recruitment and Selection Data
- Salary Review
- Training Scheduling Data
- e-Learning Data
- Succession and Career Planning Data
- Leave Data
- Graphical Dashboards

13. Collection and Transfer of Personal Information

Personal information is collected in the following ways:

- Receiving personal data through WeTransfer or similar software
- Receiving personal data in the format of a password-protected Excel file. The applicable password is sent to Signify in a separate email, SMS or WhatsApp message
- Receiving personal data through automated data imports:
    - Receiving csv files by retrieving them from SFTP or FTPS folders
    - Client pushes data to the Signify API

- For on-premises installations, clients can directly populate the relevant staging tables in the Signify database
- Also for on-premises installations, the data can be retrieved from a different database on the network and imported into Signify

- Client being advised not to send any personal information in any other format than described above

14. Storage of Personal Information

All personal information collected from a client is stored as follows:

- On a Signify internal file server (Adriano)
- In sent items in a Signify-owned mailbox
- On SharePoint

Personal information is kept for no longer than is necessary.

No personal information is allowed to be stored on any device other than those mentioned above.

15. Deletion of Personal Information

All personal information collected from a client is deleted during the decommissioning of a Signify System.

The following deletion processes apply:

- Temporary deletion
  - The client's Signify System is decommissioned.
  - The Signify database and web files are removed, but backups are retained on the server for a pre-defined period.
  - Access to personal information available to Signify System infrastructure.

- Permanent deletion

The Signify database, web files, and all backups (including web and database backups) are permanently deleted from the server. No backups are retained.

16. Data retention and deletion during the lifetime of the client's subscription

While a client's subscription is active, data cleanup is necessary from time to time to maintain space on the hosting infrastructure. The following guidelines are followed in this regard:

Type of data	Retention
Operational data – any data captured on the system by the client	No operational data of active modules will be deleted, unless requested by the client on a case-by-case basis.
Audit and import backup data – during the normal use of the system operational data is modified and an audit trail is kept of the changes made. Additionally on system imports the data imported is backed up.	Such audit and backup data will; be retained for a period of 1 year, after which it may be deleted.

IMPORTANT: When a client cancel's their subscription of our service, all data linked to the subscription will be permanently deleted from our hosting servers within 3 months of cancellation, or immediately if requested by the client.

17. Disposal of Media

At the end of the information management life cycle, the secure disposal and/or reuse of media is critical to preventing accidental unauthorised disclosure or the misuse of information and to prevent a breach of confidentiality.

The following needs to be done to ensure information is protected from breaches in confidentiality through the correct erasure, decommissioning or destruction processes whenever it is to be reused or reaches its end of life.

Hard copy media

- All office paper waste classified as public that originates from within the organisation will be shredded using a cross-cut shredder.

Optical media

- CDs and DVDs should be shredded using a cross-cut shredder.

Magnetic media

- Data must be erased using approved secure-erasure software prior to reuse or disposal. The currently approved software is Eraser. A copy is available on our local file server (*adriano.signify.local**FileServer**CDRack**Eraser*).
- At the end of life, hard drives, SSDs, USB sticks and flash drives must be destroyed by an approved and certified organisation.

- When magnetic or USB media are not accessible to perform the erase using the Eraser software, it should be physically destroyed before handing over to e-Waste.

Leased equipment

- In cases like this, the leasing company is responsible for the secure erasure or destruction of the data. Confirmation must be received from them that the erasure or destruction has been completed after the return of the equipment to the leasing company.

Use of third-party secure destruction services

- Signify currently uses the Mega IT Store as our e-Waste partner.
- Upon destruction, the Mega IT Store supplies Signify Software with a destruction certificate.
- A copy of the destruction certificate is kept on SharePoint.

18. Roles and Responsibilities

Note: The names of the individuals linked to the below roles can be found in the 'Organisational Controls' document

Role	Responsibilities:
Chief Information Security Officer (CISO) or Senior Information Risk Owner (SIRO)	• Assumes full accountability for the information controlled and processed by the organisation, including PII. • Is the face and figurehead of the organisation to interested parties. Holds a significant position in the organisation, giving confidence to those parties that the organisation takes data protection and information security seriously.
Data Protection Officer	• Keeps the Board updated on data protection responsibilities, risks and issues. • Reviews all data protection procedures and policies on a regular basis. • Arranges data protection training and advice for all staff members and those included in this policy. • Answers questions on data protection from staff, Board members and other stakeholders. • Responds to individuals such as clients and employees who wish to know which data is being held on them by Signify.

	• Checks and approves with third parties that handle the Company's data, and any contracts or agreements regarding data processing.
Information Security Manager	• Ensures that information security risks have been identified and assessed, taking account any special requirements for personal data. • Supports and advises other responsible managers and individuals regarding information security requirements, policies and controls.
Infrastructure Manager	• Ensures all systems, services, software and equipment meet acceptable security standards. • Regularly checks and scans security hardware and software to ensure it is functioning properly. • Researches third-party services, such as cloud services that the Company is considering using to store or process data.
Marketing Manager	• Approves data protection statements attached to emails and other marketing. • Addresses data protection queries from clients, target audiences or media outlets. • Coordinates with the Data Protection Officer to ensure all marketing initiatives adhere to data protection laws and the Company's Data Protection Policy. • Complies with other legislation and regulations relevant to data protection in marketing activities.

19. Staff Responsibility

All individual staff members are responsible for playing their part in maintaining the confidentiality, integrity, and availability of personal data in compliance with the POPIA (Protection of Personal information Act), GDPR (General Data Protection Regulation), DPA (Data Processing Agreements) and organisational policies, standards, and procedures.

Each person must familiarise themselves with the requirements contained in this policy and any other relevant security policy and comply with any requirements on the proper handling and security of personal data.

Your own personal data

Each staff member must take reasonable steps to ensure that the personal data Signify holds about them is accurate and updated as required. For example, if a person's personal circumstances change, they should inform the Data Protection Officer (DPO) or the HR Department so that their records can be updated. If available, they can update their personal information using the HR system's employee self-service functionality.

Handling others' personal data

All employees must familiarise themselves with the organisational responsibilities detailed above and ensure that they comply with these whenever they are handling personal data. Special care and attention must be given when handling sensitive personal data.

Processing data in accordance with the individual's rights

Staff members must abide by any request from an individual not to use their personal data for direct marketing purposes. Notify the Data Protection Officer (DPO) about any such request if it falls outside of the normal processes or if there is reason to be unsure about the appropriate practice.

Contact the Data Protection Officer for advice on direct marketing before starting any new direct marketing activity to ensure compliance with all relevant data protection and other legislation.

Reporting breaches

All employees have an obligation to report actual or potential data protection weaknesses, events, and incidents where compliance may be breached.

This allows us to do the following:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures.

The reporting of such weaknesses, events and incidents will be managed through our Information Security Incident Management processes (refer to *MNMT-PROC-03_Signify Incidents_NC CA*).

Monitoring

All staff members, suppliers and contractors must observe this policy, although the Data Protection Officer has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

20. Our Data Protections and Privacy Commitment

Data protection and privacy matters to us and we know it matters to our clients. We are committed to protecting our clients' privacy, keeping their personal information safe, and ensuring the security of their personal information.

To provide clients with the most effective products and services, their personal information will be collected, processed lawfully, stored securely and not disclosed unlawfully to any third party.

21. Compliance

Management will continuously monitor and assess compliance against this policy. Any noncompliance with or breach of this policy may lead to investigation and action in line with the organisation's disciplinary process (*control 6.4*).

22. Process Outputs

Records	Responsible	Retention	Disposition
Email correspondence	BE Manager	Retained as soft copy on Signify network no longer than required	Delete any personal information as soon as the intended purpose has been achieved.
Files sent via WeTransfer	BE Manager	Retained as soft copy on Signify network no longer than required	Delete any personal information as soon as the intended purpose has been achieved.

Excel files	BE Manager	Retained as soft copy on Signify network no longer than required	Delete any personal information as soon as the intended purpose has been achieved.
Signify System	Database Administrator	Retained as soft copy on Signify network no longer than required	Delete any personal information as soon as the intended purpose has been achieved.