Signify Privacy Rules

Signify confidential

Contact details
Signify Privacy Office
The Edge Amsterdam West, 5th Floor
Basisweg 10
1043 AP Amsterdam

Version history

Date	*Updated sections*	*Version*
19 July 2017	New Philips Lighting version	1.0
21 November 2018	Update for new WP256 requirements	
24 September 2019	Update for Signify name change	
14 August 2020	Update based upon AP feedback	
12 August 2021	Update to scope	
3 January 2022	Company address change	

Introduction

Protecting the Personal Data of individuals (e.g. consumers, business customers, employees, job applicants, and other natural persons) is a top priority for Signify.

These Signify Privacy Rules (henceforth the "Privacy Rules") have two main purposes:

1. establishing a uniform, adequate and global regulatory framework for the Processing of Personal Data within Signify;
2. establishing adequate protection for the transfer of Personal Data inside and outside Signify.

The Signify Privacy Rules constitute an integral part of the Signify Integrity code (the "Integrity code") and any case of non-compliance with the Privacy Rules is considered to be a violation of the Integrity code and may result in disciplinary actions.

Article 1. Scope and Applicability

Scope	**1.1**	These Privacy Rules apply to all Group Companies that act as a Controller of Personal Data that are (i) subject to the data transfer restrictions under the data protection laws of the European Economic Area (collectively, EEA Data Protection Laws), and (ii) transferred to a Group Company in a country outside the EEA for which there is no Adequacy Decision. A full list of the Group Companies is available here. These Privacy Rules do not apply to the Processing of information or set of information that does not qualify as Personal Data (e.g., information exclusively related to weather conditions, climate, energy saving, light efficiency, etc. that cannot identify, even indirectly, any Individuals). Signify may supplement these Privacy Rules through sub-policies, guidelines and procedures that are consistent with these Privacy Rules.
Description of the transfers of Personal Data	**1.2**	Within Signify, the exchange of Personal Data processed by Group Companies as Controllers, may take place between: a) Group Companies established worldwide. b) Group Companies and Third Parties established worldwide. Personal Data are transferred and/or processed for business purposes including, but not limited to:

Purposes for which Personal Data of consumers, business customers, suppliers, business partners and other natural persons (such as research participants) may be transferred or processed

- **Assessment and acceptance of a customer, consumer, supplier or business partner.**
  This purpose includes the Processing of Personal Data in connection with the assessment and acceptance of certain third parties (such as consumers, business customers, suppliers, business partners), including confirming and verifying the identity of relevant Individuals (which may include the use of a credit reference agency or other third party), conducting due diligence and screening against publicly available government and/or law enforcement agency sanction lists and other third-party data sources, using and participating in Signify's incident registers and sector warning systems and/or third party verification services.
- **Conclusion and execution of agreements and settlement of payment transactions.**
  This purpose includes the Processing of Personal Data in connection with the conclusion and execution of agreements, and includes activities such as sales, billing (incl. settlement of payment transactions), shipment of products or services, registration to mobile applications or websites, warranty, service communications, account management.
- **Assistance of a customer, consumer, supplier or business partner.**
  This purpose includes the Processing of Personal Data in connection with providing support, upon request (e.g. customer service).
- **Business process execution, internal management and management reporting.**
  This purpose includes the Processing of Personal Data in connection with activities such as management of company assets (including IT systems and infrastructure), finance and accounting, credit assessment (including setting credit limits) and risk management, conducting (internal) audits and investigations, implementing business controls, provision of central Processing facilities for efficiency purposes, management of alliances, ventures, mergers, acquisitions and divestitures, re-organizations or disposals and integration with purchaser, management reporting and analysis,

archive and insurance purposes, legal or business consulting, government and legal affairs, intellectual property management.

- **Relationship management and direct marketing.**
  This purpose includes the Processing of Personal Data in connection with activities such as maintaining and promoting contact, investor relations, external communications, account management, product-recalls, execution and analysis of market surveys and marketing strategies, execution of direct marketing communications.
- **Development and improvement of applications, products and/or services.**
  This purpose includes the Processing of Personal Data in connection with the development and improvement of Signify's products, systems and/or services and for research and development.
- **Security and protection of interests and/or assets of Signify**.
  This purpose includes the Processing of Personal Data in connection with the security and protection of the interests and/or assets of Signify and its consumers, business customers and business partners, including the safeguarding of the security and integrity of their business sector. In particular, it includes activities such as detecting, preventing, investigating and combating (attempted) criminal or objectionable conduct directed against Signify, its employees or customers (including the use of and participation in Signify's incident registers and sector warning systems), activities such as those involving health and safety, authentication of customer, supplier or business partner status and access rights (such as required screening activities for access to Signify's premises or systems), and activities such as deploying and maintaining technical and organizational security measures.
- **Compliance with legal obligations**.
  This purpose includes the Processing of Personal Data in connection with the performance of a task carried out to comply with a legal obligation to which Signify is subject, including the disclosure of Personal Data to government institutions or supervisory authorities, including tax authorities and other competent authorities for the sector in which Signify operates.
- **Protection of the vital interests of individuals.**

This purpose includes the Processing of Personal Data in connection with the protection of the vital interests of an individual.

- **Defense of legal claims.**
  This purpose includes the Processing of Personal Data in connection with activities such as preventing, preparing for or engaging in dispute resolution.

Purposes for which Personal Data of job applicants or Employees may be transferred or processed

- **Assessment and acceptance of job applicants.**
  This purpose includes the Processing of Personal Data in connection with recruitment activities, such as the evaluation of job applicants (including identifying and evaluating candidature, assessing skills, qualifications and interest in the context of Signify career opportunities, conducting background checks and assessments as required or permitted by applicable local law).
- **Human Resources and Personnel Management**
  This purpose includes the Processing of Personal Data in connection with activities such as concluding and executing employment-related agreements with Employees, managing the employment relationship, (e.g. administration of outplacement, employability, leave and other absences, compensation and benefits, including pensions and/or shares, tax issues, career and talent development, performance evaluations, training, disciplinary matters, grievances and terminations, business travel, expenses and reimbursements).
- **Assistance of job applicants or Employees.**
  This purpose addresses the Processing of Personal Data in connection with providing support to job applicants or Employees, upon request (e.g. helpdesk services).
- **Business process execution, internal management and management reporting.**
  This purpose includes the Processing of Personal Data in connection with activities such as internal communications, scheduling work, recording time, managing company and employee assets (including the IT systems and infrastructure), provision of central Processing facilities for efficiency purposes, conducting (internal) audits and investigations, performing internal surveys, implementing business controls, finance and accounting, management

reporting and analysis, managing and using employee directories, managing courses and/or trainings, managing projects and costs, managing alliances, ventures, mergers, acquisitions and/or divestitures, re-organizations or disposals and integration with purchaser, archive and insurance purposes, legal or business consulting, budgeting, financial management and reporting, communications.

- **Employee communications (incl. direct marketing).**
  This purpose includes the Processing of Personal Data in connection with activities such as communications around specific employee discounts or invitations for charity initiatives and other events.
- **Security and protection of interests and/or assets of Signify**.
  This purpose includes the Processing of Personal Data in connection with the security and protection of the interests and/or assets of Signify and its Employees in the sector in which Signify operates. In particular, it includes activities such as the screening and monitoring of Employees before and during employment, the screening against publicly available government and/or law enforcement agency sanction lists and other third-party data sources, the detecting, preventing, investigating and combating (attempted) fraud and other criminal or objectionable conduct (including the use of and participation in Signify's incident registers and sector warning systems) and activities such as occupational health and safety, authentication of job applicants and Employee status and access rights, deploying and maintaining technical and organizational security measures.
- **Development and improvement of applications, products and/or services.**
  This purpose includes the Processing of Personal Data in connection with the development and improvement of Signify' products, systems and/or services and for research and development.
- **Compliance with legal obligations**.
  This purpose includes the Processing of Personal Data in connection with the performance of a task carried out to comply with a legal obligation to which Signify is subject, including the disclosure of Personal Data to government institutions or supervisory authorities, including tax authorities and other competent authorities for the sector in which Signify operates.

		▪ **Protection of the vital interests of individuals.** This purpose includes the Processing of Personal Data in connection with the protection of the vital interests of an individual. ▪ **Defense of legal claims.** This purpose includes the Processing of Personal Data in connection with activities such as preventing, preparing for or engaging in dispute resolution.
Relation between these Privacy Rules and Applicable Data Protection Law	**1.3**	These Privacy Rules provide supplemental rights and remedies to Individuals only. Nothing in these Privacy Rules will be construed to take away any rights or remedies that Individuals may have under applicable local law. In case a Group Company has reasons to believe that Applicable Data Protection Law prevents such company from fulfilling its obligations under these Rules and has substantial effect on the safeguards provided by these Privacy Rules or in case there is a conflict between Applicable Data Protection Law and these Privacy Rules, the relevant Group Company shall inform the Signify central Privacy Office (except when prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). The Signify central Privacy Office (in consultation with Signify Group Legal) will advise on how to proceed on a case-by-case basis. Subject to the following paragraph, Signify shall inform the competent Data Protection Authority if Signify becomes aware that applicable local law of a non-EEA country is likely to have a substantial adverse effect on the protection offered by these Privacy Rules, including if Signify receives a legally binding request for disclosure of Personal Data from a law enforcement authority or state security body of a non-EEA country (**Disclosure Request**). Notifications of a Disclosure Request shall include information about the data requested, the requesting body, and the legal basis for the disclosure. If notification of a Disclosure Request is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, Signify will request the relevant authority to waive this prohibition and will document that it has made this request. In any event, Signify will on an annual basis provide to the lead Data Protection Authority general information on the number and type of Disclosure Requests it received in the preceding 12

		month period, to the fullest extent permitted by applicable law. In any event, any transfers by Signify of Personal Data in response to a Disclosure Request will not be massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society. This Article does not apply to requests received by Signify from other government agencies in the normal course of its activities, which Signify can continue to provide in accordance with applicable law.

Article 2. Privacy Principles

As general principle, Signify shall not collect and further process Personal Data if its intended business purposes can be reasonably fulfilled without Processing Personal Data. Signify shall process Personal Data lawfully, fairly and in a transparent manner.

When Processing Personal Data, Signify shall respect the "Privacy Principles" set out hereinafter.

Legal basis for Processing Personal Data	**2.1**	The Processing of Personal Data is only permitted if at least one of the following legal bases apply: a) the Individual has given his/her Consent in relation to one or more specific purposes; or b) the Processing of Personal Data is necessary to establish a contractual relationship with the Individual (including taking steps prior to entering into a contract); or c) the Processing of Personal Data is necessary to pursue the legitimate interest of Signify, except where such interest is overridden by the interest or data protection rights of the Individual; or d) the Processing of Personal Data is necessary for compliance with a legal obligation to which Signify is subject; or e) the Processing of Personal Data is necessary in order to protect the vital interests of the Individual or of another individual.
Employee's Consent	**2.2**	Employee Consent generally cannot serve as a legitimate basis for Processing Personal Data of Employees, unless: a) such Consent is required by applicable law; or

		b) such Processing is considered by Signify to be in the interest or for the benefit of the Employee; or c) where Consent is otherwise appropriate in view of the privacy interests of the Employee.
Consent and Individual's choice	**2.3**	Where Consent has been granted, the Individual may withdraw such Consent at all times. Withdrawal of Consent for the Individual shall be as easy as it was to grant Consent. In case of withdrawal, Signify shall cease the Processing of Personal Data without undue delay upon receipt of such withdrawal. The withdrawal of Consent shall not affect the lawfulness of the Processing of Personal Data based on such Consent before its withdrawal. When seeking consent, Signify must inform the Individual: a) of the purposes of the Processing for which consent is required; b) of the right to withdraw his or her consent at any time; c) that withdrawal of consent does not affect the lawfulness of the relevant Processing before such withdrawal.
Purpose limitation	**2.4**	Personal Data shall be Processed for specified, explicit and business purposes. Furthermore, Personal Data shall not be Processed in a way incompatible with the business purposes for which they were originally collected. Personal Data may be Processed for other business purposes (different from the one for which they were originally collected, **Secondary Purpose**) only if the Secondary Purpose is closely related ('compatible') to the business purpose(s) for which they were originally collected. For example, it is generally permissible to Process Personal Data for the following purposes: • anonymization of Personal Data; • transfer of Personal Data to an archive; • internal audits or investigations; • implementation of business controls and operational efficiency; • IT systems and infrastructure related Processing such as for maintenance, support, life-cycle management, and security (including resilience and incident management);

		• statistical, historical or scientific research; • dispute resolution; • legal or business consulting; or • insurance purposes. Before Processing Personal Data for a Secondary Purpose, Staff shall seek the advice of the appropriate Privacy Officer. Depending on the sensitivity of the relevant Personal Data and whether use of the Personal Data for the Secondary Purpose has potential negative consequences for the Individual, such use may require additional measures such as: a) limiting access to the Personal Data; b) imposing additional confidentiality requirements; c) taking additional security measures, including encryption or pseudonymization; d) informing the Individual about the Secondary Purpose; e) providing an opt-out opportunity to the Individual; or f) obtaining the Individual's Consent.
Data minimization	**2.5**	Signify shall limit the Processing of Personal Data to those Personal Data that are reasonably adequate for and relevant to its business purposes (data minimization).
Data quality	**2.6**	Personal Data shall be accurate, complete and kept up to date to the extent reasonably necessary for the applicable business purpose. Signify shall take reasonable steps to (i) delete, de-identify or destroy (e.g., by scrambling) Personal Data that is not required for the applicable business purpose in accordance with Article 2.7, and (ii) rectify Personal Data that is inaccurate. Signify shall facilitate Individuals in ensuring that their Personal Data are accurate, complete and up-to-date, in accordance with Article 2.9.
Storage limitation	**2.7**	Signify shall retain Personal Data in accordance with its data and records retention schedules that define the appropriate retention periods, taking into account: a) for the period required to serve the respective business purposes; b) to the extent reasonably necessary to comply with an applicable legal requirement; or c) as advisable in light of an applicable statute of limitations.

		Unless differently required by applicable local law, Personal Data which are no longer required to serve the business purposes for which they were originally collected, shall promptly be anonymized or destroyed. Signify shall specify (e.g. in specific sub-policies or procedures) the time periods for which certain categories of Personal Data may be kept, before being destroyed, or anonymized.
Sensitive Data	**2.8**	Signify will only Process Criminal Data where permissible under applicable law and to the extent necessary to serve the applicable Business Purpose. The Processing of Special Categories of Personal Data is prohibited unless one or more of the grounds below apply: a) The Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Signify or of the Individual in the field of employment and social security or as required or permitted under applicable local law; or b) The Processing is necessary to protect the vital interests of the Individual or of another person where the Individual is physically or legally incapable of giving his Consent; or c) The Processing relates to information which are manifestly made public by the Individual; or d) The Processing is necessary for the establishment, exercise or defense of legal claims. e) Signify has obtained the Individual's explicit Consent (if required by local applicable law).
Privacy rights of Individuals (including complaint handling process)	**2.9**	According to these Privacy Rules, the Individual has the right to: a) obtain a copy of these Privacy Rules (upon request); b) obtain confirmation as to whether or not Personal Data concerning him or her are being processed by Signify and/or Third Parties on behalf of Signify; c) access to the information listed in Article 3.1 about his/her Personal Data; d) obtain a copy of (part or all of his or her) Personal Data relating to him or her undergoing Processing by Signify, to the extent that this does not adversely affect the rights and freedoms of other Individuals; e) have his or her Personal Data rectified without undue delay, if such Personal Data are incorrect or inaccurate;

f) have his or her Personal Data anonymized or erased (unless the respective Group Company has a legal obligation to keep the Data);
g) have the Processing of his or her Personal Data restricted, to the extent provided for by EEA Data Protection Law;
h) object at any time to (i) the Processing of his or her Personal Data on grounds relating to his or her particular situation, unless Signify can demonstrate prevailing compelling legitimate grounds for the Processing; and (ii) receiving direct marketing communications (including any profiling related thereto). If the Individual objects against the processing of his or her Personal Data for direct marketing purposes, the relevant Personal Data shall no longer be processed for such purposes;
i) object to the Processing of his or her Personal Data which is based solely on automated Processing (including profiling) and which produces adverse legal effects concerning him or her;
j) contact, at any time, Signify with privacy-related questions and/or complaints regarding the application or violation of these Privacy Rules by a Group Company; and
k) make use of his or her third party beneficiary rights and/or claim damages as described in Article 5.1.

The above rights of Individuals do not apply if the exercise of such right by the Individuals adversely affects the rights and freedoms of others.

The Individual's right to erasure and the right to correction do not apply in one or more of the following circumstances:
a) the Processing is necessary for compliance with a legal obligation of Signify; or
b) the Processing is necessary for a task carried out in the public interest, including in the area of public health; or
c) the Processing is necessary for archiving, scientific or historical research or statistical purposes; or
d) the Processing is necessary for exercising the right of freedom of expression and information; or
e) the Processing is necessary for dispute resolution purposes.

The Individual can exercise the above rights by sending a written request to the contact person or contact point indicated by Signify in the relevant privacy notice.

Prior to fulfilling the request of the Individual, Signify may require the Individual to:

a) show proof of his or her identity; and
b) where Signify Processes a large amount of Personal Data concerning the Individual, specify the information or Processing activities to which the request relates.

Without undue delay, and in any event within one month of the receipt of the request or complaint (if no EEA Data Protection Law defines a shorter timeframe), Signify will inform the Individual in writing either:

a) of Signify position with regard to the request or complaint and any action it has taken or will take in response; or
b) the ultimate date on which the Individual will be informed of Signify position, which date shall – taking into account the complexity and volume of requests Signify has at any point – be no later than two months thereafter.

Signify may deny the request of the Individual only in the following cases:

a) the request is not in a written form; or
b) the request is not sufficiently clear and/or specific; or
c) the identity of the Individual cannot be established by reasonable means; or
d) the request is manifestly unfounded or excessive (for example because it constitutes an abuse or rights or because of its repetitive character); or
e) the request is covered by legal professional privilege; or
f) the request violates the rights of other individuals; or
g) the request violates any other local applicable law.

Where the Individual makes the request in electronic form, the information requested will be provided in an electronic form, unless otherwise requested by the Individual. Signify is not obliged to Process additional information in order to be able to identify the Individual for the sole purpose of facilitating the rights of the individual under this Article 2.9.

Security and confidentiality	**2.10**	*Security measures for the protection of Personal Data* Personal Data shall be protected against misuse or accidental, unlawful, or unauthorized destruction, loss,

alteration, disclosure, acquisition or access, using commercially reasonable technical, physical and/or organizational measures. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks that the Processing of Personal Data may pose to the Individuals.

In assessing the appropriate level of security, Signify takes into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

Sensitive Data shall be processed with enhanced security measures.

For example, where appropriate, these security measures shall include:

a) the pseudonymization and encryption of Personal Data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

Data Security Breach

Signify shall document any Data Security Breaches, comprising the facts relating to the incident, its effects and the remedial actions taken, which documentation will be made available to the competent Data Protection Authority upon request. Group Companies shall inform Signify Netherlands B.V. of a Data Security Breach without delay.

In addition, Signify will notify any Data Security Breaches:

- to the competent Data Protection Authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the Data Security Breach is unlikely to result in a risk to the rights and freedoms of Individuals; and

- to Individuals without undue delay, if the Data Security Breach is likely to result in a high risk to the rights and freedoms of such Individuals.

Signify shall respond promptly to inquiries of affected Individuals relating to such Data Security Breach

Confidentiality

Personal Data shall be accessed and processed only by personnel who is authorized and has been specifically instructed to do so. Personnel who access Personal Data:

- shall be authorized to access Personal Data only to the extent strictly necessary to serve the applicable business purpose and to perform their job;
- shall have imposed written confidentiality obligations.

Records of Processing activities

Signify shall maintain a record of Processing activities under its responsibility (e.g. inventory of systems and databases Processing Personal Data). Insofar as required by EEA Data Protection Law, this record shall in any event contain information about:

a) the name and contact details of the relevant Controller;
b) the purposes of the Processing;
c) the categories of Individuals and of the categories of Personal Data;
d) the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organizations;
e) where applicable, transfers of Personal Data to non-EEA countries for which the European Commission has not issued a decision regarding the adequacy of the non-EEA country's level of protection of Personal Data including the identification of that non-EEA country, and, where applicable, documentation of suitable safeguards;
f) where possible, the envisaged retention periods; and
g) where possible, a general description of the technical and organizational security measures referred to in this Article 2.10.

A copy of this record will be provided to the Data Protection Authority upon request.

		Data Protection Impact Assessment Signify shall maintain a procedure to conduct and document a prior assessment of the impact which a given Processing may have on the protection of Personal Data, where such Processing is likely to result in a high risk for the rights and freedoms of Individuals, in particular where new technologies are used (Data Protection Impact Assessment) ("**DPIA**"). Where the DPIA shows that, despite mitigating measures taken by Signify, the Processing still presents a residual high risk for the rights and freedoms of Customers, the Lead DPA will be consulted prior to such Processing taking place.
Privacy by design and by default	**2.11**	During the development and/or designing of new products, applications, services or systems that are either based on the Processing of Personal Data or that process Personal Data to fulfil their task – and taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of Processing of Personal Data – Signify shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of Individuals, take efforts to integrate into the developing and designing process of the aforementioned new products, applications, services or systems the necessary privacy safeguards and controls in order to meet the requirements set forth in Art. 2.5, 2.6, 2.7 and 2.9 of these Privacy Rules.

Article 3. Privacy Fundamentals

When Processing Personal Data, Signify shall respect the "Privacy Fundamentals" set out hereinafter.

Phase 1 - Collection of Personal Data

Information to be provided to the Individuals (Privacy Notice)	**3.1**	At the time when Personal Data are obtained, Signify shall provide the Individual with a Privacy Notice containing, at least, the following information: a) the identity of the relevant Controller; b) the contact details of the central Privacy Office; c) the purposes for which his or her Personal Data are transferred and further processed, and the legal basis for such Processing;

d) where the Processing is based on Signify's or a third party's legitimate interests, the pursued legitimate interest;
e) the recipients or categories of recipients of the Personal Data;
f) the categories of third parties to which Personal Data will be disclosed; whether the third party is located in a non-adequate county; and (where applicable and required) the appropriate safeguard used to transfer such Personal Data to such third party, as well as the means to get a copy thereof, or access thereto;
g) the rights of Individuals (as identified in Article 2.9 of these Privacy Rules);
h) other relevant information to the extent reasonably required to make the Individual aware about how Signify intends to use his or her Personal Data, e.g.:
    - the nature and categories of the Personal Data Processed;
    - the period for which the Personal Data will be stored or (if not possible) the criteria used to determine this period;
    - an overview of the rights of Individuals under these Privacy Rules and how these can be exercised, including the right to withdraw consent in accordance with Article 2.3, to obtain compensation, and to lodge a complaint with a Data Protection Authority;
    - the existence of automated decision making referred to in Article 3.5 as well as meaningful information about the logic involved and potential negative consequences thereof for the Individual; and/or
    - the source of the Personal Data (where Personal Data have not been obtained from the Individual), including whether the Personal Data came from a public source.

This information shall be provided in a clear and comprehensible manner, for example, by means of privacy notices and/or by making use of appropriate icons and symbols.

As an exception, this information does not have to be provided if:

a) the Individual already has the information referenced above about the intended Processing;

b) the provision of the above information proves impossible or would involve a disproportionate effort.

Phase 2 – Transfer of Personal Data

Transfer of Personal Data inside the Signify Group	**3.2**	If a Group Company intends to involve another Group Company to Process Personal Data on its behalf, the latter undertakes to: a) Process Personal Data only in accordance with the instructions and for the purposes authorized by the Group Company (Controller) on whose behalf the Processing is carried out; and b) Process Personal Data in compliance with these Privacy Rules. Unless differently required by EEA Data Protection Law, the transfer of Personal Data to and between the Group Companies is governed and covered by these Privacy Rules.
Transfer of Personal Data outside the Signify Group	**3.3**	*Outsourcing the Processing of Personal Data (to Third Parties acting as Processors)* If a Group Company intends to outsource and/or commission the Processing of Personal Data to a Third Party acting as Processor, the following requirements must be observed: a) Signify shall only engage a Third Party Processor to the extent necessary to serve the applicable business purpose. b) The Third Party Processors shall be carefully selected. A Third Party Processor shall be selected who is able to ensure the necessary technical and organizational security measures required to process Personal Data in compliance with these Privacy Rules and Applicable Data Protection Law. The performance of the Processing of Personal Data commissioned and/or outsourced to the Third Party Processor must be regulated by a written contract between Signify and the Third Party Processor in which the rights of the Individuals are safeguarded and the obligations of the Third Party Processor clearly defined (the "Data Processor Agreement"). In addition to any provisions specifically

required by EEA Data Protection Law, such Data Processor Agreement shall, at least, include provisions ensuring that:

a) the Third Party Processor will process Personal Data only in accordance with Signify's documented instructions and for the purposes authorized by Signify, including on transfers of Personal Data to any Third Party Processor not covered by an Adequacy Decision, unless the Third Party Processor is required to do so under mandatory requirements applicable to the Third Party Processor and notified to Signify;
b) the Third Party Processor will take the appropriate technical, physical and organizational security measures to protect Personal Data and shall promptly inform Signify of a Data Security Breach involving Personal Data;
c) the Third Party Processor shall keep the Personal Data confidential and ensures that staff with access to Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
d) the Third Party Processor shall only permit subcontractors to Process Personal Data in connection with its obligations to Signify (a) with the prior specific or generic Consent of Signify and (b) based on a validly entered written or electronic contract with the subcontractor, which imposes similar privacy protection-related Processing terms as those imposed on the Third Party Processor under the Data Processor Agreement with Signify and provided that the Third Party Processor remains liable to Signify for the performance of the subcontractors in accordance with the terms of the Data Processor Agreement. If Signify provides generic consent for involvement of subcontractors, the Third Party Processors shall provide notice to Signify of any changes in its subcontractors and will provide Signify the opportunity to object to such changes based on reasonable grounds;
e) the Third Party Processor shall make available to Signify the information necessary to demonstrate compliance with its obligations under the Data Processor Agreement and further (a) submit its relevant information processing facilities to audits and inspections by Signify, a Third Party on behalf of Signify, or any relevant public authority, or (b) periodically make available to Signify a statement issued by a qualified independent third party

assessor on behalf of Third Party Processor certifying that the information processing facilities of the Third Party Processor used for the Processing of Personal Data comply with the requirements of the Data Processor Agreement;

f) the Third Party Processor shall deal promptly and appropriately with (a) requests and complaints of Individuals as instructed by Signify; and (b) requests for assistance of Signify as reasonably required to ensure compliance of the processing of the Personal Data with Applicable Data Protection Law; and
g) Upon termination of the Data Processor Agreement, the Third Party Processor shall, at the option of Signify, return the Personal Data and copies thereof to Signify or shall securely delete such Personal Data, except to the extent the Data Processor Agreement or applicable law provides otherwise.

Internal Processors may process Personal Data only if they have a validly entered into written or electronic contract with the Group Company being the Controller of the relevant Personal Data, which contract must in any event include the provisions set out above.

Data Transfers to Third Parties outside the EEA

Personal Data may be transferred to a Third Party that is located outside the EEA and not covered by an Adequacy Decision if:

a) Signify and the relevant Third Party have entered into (a) standard data protection clauses adopted by the European Commission, or (b) standard data protection clauses adopted by a Data Protection Authority and approved by the European Commission;
b) the Third Party has been certified under an approved mechanism that is recognized under applicable EEA Data Protection Laws as providing an "adequate" level of privacy protection;
c) the Third Party has implemented Binding Corporate Rules or a similar transfer control mechanism that is recognized under applicable EEA Data Protection Laws as providing an "adequate" level of privacy protection;
d) the transfer has been approved by the relevant Privacy Officer and is necessary:
    a. for the performance or management of a contract with the Individual, or for taking

		necessary steps at the request of the Individual prior to entering into a contract, e.g., for processing orders; b. for the conclusion or performance of a contract concluded in the interest of the Individual between Signify and a Third Party; c. to protect a vital interest of an individual; d. for the establishment, exercise or defense of a legal claim; e. is necessary to satisfy a pressing need to protect the public interests of a democratic society; or f. is necessary for the performance of a task carried out to comply with a legal obligation to which the relevant Group Company is subject.

Phase 3 – Use of Personal Data

Direct marketing	**3.4**	The Processing of Personal Data for direct marketing purposes (e.g. contacting individual by email, phone, SMS, social media or otherwise, with a view of solicitation for commercial or charitable purposes) shall comply with the following requirements: a) If EEA Data Protection Law so requires, Signify can only send direct marketing communications with the prior Consent (opt-in) of the Individual. b) In every direct marketing communication that is made to the Individual, the Individual shall explicitly be offered the opportunity to object to further direct marketing communications, including profiling (to the extent that the direct marketing communication is based on profiling). c) If an Individual objects to receiving direct marketing communications from Signify, or withdraws his or her Consent to receive such materials, Signify shall, as soon as possible, take steps to refrain from sending further direct marketing communications as specifically requested by the Individual. Signify will do so without undue delay. d) No Personal Data shall be provided to Third Parties for Third Parties' own direct marketing purposes without the prior Consent of the Individual to do so.
Automated individual	**3.5**	The Processing of Personal Data for the purpose of evaluating or making decisions about Individuals (including

decision making		profiling) which significantly negatively affects them shall not be solely based on automated Processing (e.g. exclusively based on the use of information technology). This restriction does not apply if: a) the Processing is based on the Individual's explicit Consent; b) the decision is necessary in the context of entering into or performing and/or managing a contract; or c) the use of automated Processing is required or authorized by EEA Data Protection Law.
Overriding interests	**3.6**	The obligations of Signify or rights of Individuals as specified in Article 3.7 of these Privacy Rules may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Individual (Overriding Interest). An Overriding Interest exists if there is a need to: a) protect the legitimate business interests of Signify, including: 1. the health, security or safety of the Employees or other Individuals; 2. its intellectual property rights, trade secrets or reputation; 3. the continuity of its business operations; 4. the preservation of confidentiality in a proposed sale, merger or acquisition of a business; or 5. the involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes; b) prevent or investigate (including cooperating with law enforcement) suspected or actual violations of law, contracts or other Signify policies; c) protect or defend the rights and freedoms of Signify, its Employees or other individuals.
Exceptions in the event of Overriding Interests	**3.7**	If an Overriding Interest exists, one or more of the following obligations of Signify or rights of the Individual may be set aside: a) Article 2.4 (Purpose Limitation) b) Art. 2.7 (Storage limitation) c) Art. 2.9 (Privacy rights of individuals) d) Art. 2.10 (Security and confidentiality) e) Art. 3.1 (Information to be provided to the Individuals) f) Art. 3.3 (Transfer of Personal Data outside the Signify Group)

		The requirements of Article 2.8 (Sensitive Data) may be set aside only for the Overriding Interests listed in Article 3.6 (a) (1), (2), (3), (5) or Article 3.6 (b) or Article 3.6 (c).
Consultation and information requirements in the event of Overriding Interests	**3.8**	Setting aside obligations of Signify or rights of Individuals based on an Overriding Interest, requires the prior consultation of the central Privacy Office. The central Privacy Office shall document his or her advice. Upon request of the Individual, Signify shall inform the Individual of the Overriding Interest for which obligations of Signify or rights of the Individual have been set aside, unless the particular Overriding Interest sets aside the requirements of Articles 2.9 or 3.1, in which case the request shall be denied.

Article 4. Effectiveness of the Privacy Rules

Responsibility for compliance with the Privacy Rules	**4.1**	With regards to Personal Data processed under its direct control and authority: a) each Group Company (represented by the executive management or the CEO) is responsible for compliance with the Privacy Rules and with Applicable Data Protection Law; the Group Company may delegate this task (but cannot delegate the responsibility) to appropriate personnel. b) Each Function and/or Business Group and/or Market (represented by its highest manager) is internally responsible for compliance with the Privacy Rules.
Role of Signify Netherlands B.V.	**4.2**	Signify Netherlands B.V. has been tasked by Signify Holding Company with overseeing and monitoring the group-wide implementation of these Privacy Rules.
Signify Privacy Governance	**4.3**	As part of its commitment to ensuring compliance with these Privacy Rules and to respecting Individuals' rights to privacy, Signify has established: a) a central Privacy Office, composed of a Chief Privacy Officer and qualified privacy professionals in the role of Privacy Officers. The central Privacy Office has the main tasks of overseeing and monitoring the group-wide implementation of these Privacy Rules, advising management on privacy and data protection related issues, supporting in case of interactions with Data protection Authorities,

monitoring the privacy training and handling privacy and data protection related requests and/or complaints.
The central Privacy Office will maintain an updated list of the Group Companies bound by these Privacy Rules.
The central Office is bound by secrecy or confidentiality concerning the performance of its tasks; and

b) a global network of local privacy personnel ('Privacy Contact Points') who has responsibility for supporting the relevant Group Companies to comply with these Privacy Rules.

The Chief Privacy Officer is responsible for:

(i) the development of the policies and procedures related to these Privacy Rules; and
(ii) developing and planning of awareness and/or training programs; and
(iii) monitoring and reporting, as appropriate, on compliance with these Privacy Rules to respective the management; and
(iv) coordinating the collecting, investigating and resolving privacy inquiries, concerns and complaints, and
(v) coordinating the investigation into Data Security Breach, decide in consultation with Signify Group Legal on remedial actions and notifications; and
(vi) appointment of Privacy Officer and Privacy Contact Points; and
(vii) coordinating, in consultation with Signify Group Legal, official investigations or inquiries into the Processing of Personal Data by Data protection Authorities; and
(viii) manage, oversee and facilitate Signify central Privacy Office (Central Signify Privacy Team) and Privacy Network (Global Signify Privacy Team)

The Privacy Officers are responsible for:

(i) facilitate the compliance throughout Signify with regard to the processing of the relevant Personal Data / organizations; and
(ii) spread awareness within Signify with regard to Personal Data; and
(iii) connect with the relevant organizations and manage the privacy impacts on the relevant initiatives; and

		(iv) provide support and sign-off Data Privacy Impact Assessment; and (v) coordinate the Privacy Contact Points in the relevant organizations; and (vi) regularly advise their respective executive teams and the Chief Privacy Officer on privacy risks and compliance issues; and (vii) support the implementation of the privacy compliance framework as required by the Chief Privacy Officer; and (viii) cooperate with the Chief Privacy Officer, other Privacy Officers, Privacy Contact Points, and the Integrity code Compliance Officers.
Auditing compliance with the Privacy Rules	**4.4**	To ensure that compliance with the Privacy Rules by Signify is subject to regular review, Signify will perform, at regular intervals or at the request of the central Privacy Office, an audit program which shall include any necessary corrective actions, timeframes for completing such corrective actions, and follow up to ensure that such corrective actions have been completed. The results of this audit will be communicated to the Signify Privacy Office. Any violations by a Group Company identified in the audit report will be reported to the board of management of the respective Group Company. A copy of the audit results related to compliance with the Privacy Rules will be made available, upon request, to the competent Data Protection Authority.
Training on the Privacy Rules	**4.5**	Signify will perform trainings on these Privacy Rules to personnel: a) who has permanent or regular access to Personal Data; and/or b) who is involved in the collection of Personal Data; and/or c) who is involved in the development of products and/or services used to process Personal Data.
Mutual assistance and Cooperation with Data Protection Authorities	**4.6**	All Signify Group Companies undertake to: a) assist each another and actively cooperate with the central Privacy Office in any event of suspected or identified non-compliance with these Privacy Rules by the respective Group Company and for any other issues related to the Processing of Personal Data (e.g. privacy-related requests, complaints or claims from

an Individual, investigation or inquiry by any competent government authorities, audit of compliance with the Privacy Rules, etc.).

b) cooperate with and reasonably assist each other in responding to lawful investigations or inquiries by Data Protection Authorities with regard to the implementation of these Privacy Rules, to the extent such activities take place with full respect to confidentiality and trade secrets of Signify. The competent Data Protection Authority has the authority to audit the facilities used by Signify for the Processing of Personal Data for compliance with these Privacy Rules.

c) follow the advice and recommendations of the competent Data Protection Authority with regard to the interpretation of these Privacy Rules.

Article 5. Final provisions

Third party beneficiary rights and liability

5.1 Individuals are entitled to enforce compliance with one of the following provisions of these Privacy Rules (namely: Article 1.3, Article 2.1, Article 2.4, Article 2.5, Article 2.6, Article 2.9, Article 2.10, Article 3.3, Article 3.5, Article 4.5, Article 5.1, Article 5.4) as third party beneficiaries.

To exercise the rights in respect of these provisions, Individuals are encouraged to first follow the request and complaints procedure set forth in Article 2.9 of these Privacy Rules in order to find an amicable solution with Signify.

Individuals may, at their own choice, always lodge a claim to:

a) the lead Data Protection Authority or the courts in the Netherlands, against Signify Netherlands B.V.;

b) the Data Protection Authority in the EEA country where (i) the Individual has his or her habitual residence or place of work, or (ii) the infringement took place, against the Group Company in the relevant EEA country where the infringement took place being the Controller of the relevant Personal Data; or

c) the courts in the EEA country (i) where the Individual has his or her habitual residence, or (ii) where the Group Company being the Controller of the relevant

		Personal Data is established, against such Group Company or Signify Netherlands B.V. *Liability* In case an Individual has a claim under this Article, such Individual shall be entitled to compensation of material and non-material damages suffered by that Individual resulting from a violation of these Privacy Rules to the extent provided by applicable law of the relevant EEA country. In case an Individual brings a claim for damages as set out above, it will be for the Individual to provide information that shows that he or she has suffered the relevant damages and to establish facts which show it is plausible that the damage has occurred because of a violation of these Privacy Rules. It will subsequently be for Signify to prove that the damages suffered by the Individual due to a violation of these Privacy Rules are not attributable to Signify. If an Individual brings any claims under this Art. 5.1 against Signify Netherlands B.V. for a violation of these Privacy Rules committed by a Group Company, such Group Company shall indemnify Signify Netherlands B.V. for any costs, charge, damages, expenses or loss associated with such claim.
Updating the Privacy Rules	**5.2**	Signify reserves the right to change and/or update these Privacy Rules at any time. All changes to these Privacy Rules will be communicated and/or made available without undue delay to the Group Companies. The Signify Privacy Office will maintain a list of all changes/updates to the Privacy Rules since the Privacy Rules came into force. Signify will promptly inform the lead Data Protection Authority of material changes to the Privacy Rules (if any) and coordinate Signify's responses to questions of the lead Data Protection Authority in respect thereof. Other changes (if any) will be notified by the Signify Privacy Office to the lead Data Protection Authority on a yearly basis.
Sanctions	**5.3**	Non-compliance of Employees with these Privacy Rules may result in appropriate disciplinary measures, to be taken by the relevant Group Company, in accordance with applicable local law.

Publication and taking effect	**5.4**	Signify will make the most current version of these Privacy Rules, including a list of Group Companies bound by these Privacy Rules, readily available to every Individual (e.g. by publishing these Privacy Rules on a Signify website and on the internal intranet). These Privacy Rules shall apply - for an unspecified duration - from: a) the date when the unilateral declaration or undertaking is made or given by the Signify Holding Company; or b) (when required by local law) the date when the relevant Group Company has agreed in writing to comply with these Privacy Rules;
Transitional period	**5.5**	Any entity that becomes a Group Company after these Privacy Rules take effect shall comply with these Privacy Rules within two years of becoming a Group Company. During this transition period, no Personal Data will be transferred under these Privacy Rules until (1) the relevant Group Company has achieved compliance with the Privacy Rules or (2) an alternative data transfer mechanism has been implemented, such as standard contractual clauses. A divested entity (or specific parts thereof) may remain covered by these Privacy Rules after its divestment for such period as determined by Signify to disentangle the Processing of Personal Data relating to such divested entity. Where implementation of these Privacy Rules requires updates or changes to information technology systems (including replacement of systems), the transition period shall be three years after these Privacy Rules take effect or from the date an entity becomes a Group Company, or any longer period as is reasonably necessary to complete the update, change or replacement process. Where there are existing agreements with Third Parties that are affected by these Privacy Rules, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.
Law applicable	**5.6**	These Privacy Rules shall be governed by and interpreted in accordance with Dutch law.

Definitions

The terms used in these Privacy Rules are defined as follows:

Adequacy Decision	a decision issued by the European Commission under EEA Data Protection Laws that a country or region or a category of recipients in such country or region is deemed to provide an "adequate" level of data protection.
Applicable Data Protection Law	the provisions of mandatory law of a country containing rules for the protection of individuals with regard to the Processing of Personal Data as applicable to Signify when acting as Controller.
Consent	any freely given, specific, informed and unambiguous indication of his or her wishes by which the Individual, either by a statement or by a clear affirmative action, signifies agreement to Personal Data relating to him or her being processed for particular business purposes.
Controller	Signify Holding Company and/or a Group Company which, alone or jointly with others, has the authority to make decisions with respect to the Processing of Personal Data, in particular the authority to determine the purposes and the means of the Processing of Personal Data).
Criminal Data	any Personal Data relating to criminal offenses, criminal records, or proceedings with regard to criminal or unlawful behavior.
Data Protection Authority or DPA	the public authority of a country that is responsible for monitoring the application of EEA Data Protection Law within its territory.
Data Privacy Impact Assessment	DPIA shall mean a procedure to conduct and document a prior assessment of the impact which a given Processing may have on the protection of Personal Data, where such Processing is likely to result in a high risk for the rights and freedoms of Individuals, in particular where new technologies are used. A DPIA shall contain: (i) a description of: (a) the scope and context of the Processing; (b) the Business Purposes for which Personal Data is Processed; (c) the specific purposes for which Sensitive Information is Processed; (d) categories of Personal Data recipients, including recipients not covered by an Adequacy Decision; (e) Personal Data storage periods;

	(ii) an assessment of: (a) the necessity and proportionality of the Processing; (b) the risks to the privacy rights of Individuals; and (c) the measures to mitigate these risks, including safeguards, security measures and other mechanisms (such as privacy-by-design) to ensure the protection of Personal Data.
Data Security Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
Employee	any Individual with an employment relationship with Signify. This includes temporary workers, contractors or trainees.
EEA or EEA country	the member states of the European Union (EU) and the other signatories to the Treaty on the European Economic Area (EEA).
EEA Data Protection Laws	the provisions of mandatory law of an EEA country containing rules for the protection of Individuals with regard to the Processing of Personal Information including security requirements for and the free movement of such Personal Data.
Group Company	All entities included on the List of Group Companies subject to these Privacy Rules available here which consists of: • i.e., Signify Holding Company; • companies, firms and legal entities with respect to which now or hereafter Signify Holding Company, directly or indirectly holds 50% or more of the nominal value of the issued share capital or ownership interest and/or 50% or more of the voting power at general meetings and/or has the power to appoint a majority of directors and/or to otherwise direct their activities; and • Signify associated companies in which the Signify Holding Company or a Group Company has a minority stake and which, with the approval of Signify Netherlands B.V., has given a voluntary undertaking (legally binding) to comply with these Privacy Rules; or any other natural or legal person engaged in an economic activity with a Signify Group Company (irrespective of its legal form) including partnerships or associations regularly engaged in an economic activity which, with the approval of the Signify Netherlands B.V., has given a voluntary undertaking (legally binding) to comply with these Privacy Rules.
Individual(s)	any natural person (e.g. consumer, business customer, employee, etc.) whose Personal Data is processed by Signify acting as Controller or by a Third Party on behalf of Signify.

Personal Data	any information or combination of information relating to an identified or identifiable natural person (Individual) and Processed by Signify as Controller. An identifiable 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Signify	Signify Holding Company and Group Companies.
Signify Holding Company	Signify N.V., a company registered in The Netherlands with registered number 65220692 whose registered office is at High Tech Campus 48, 5656 AE, Eindhoven, The Netherlands.
Signify Netherlands B.V.	Signify Netherlands B.V., a wholly owned company by Signify Holding Company, registered in The Netherlands with registered number 17061150 whose registered office is at High Tech Campus 48, 5656 AE, Eindhoven, The Netherlands.
Processing or Processing of Personal Data	any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Processor and Sub-Processor	any natural or legal person which processes Personal Data on behalf of the Controller. In case the Processor makes use, for the Processing of Personal Data carried out on behalf of the Controller, of affiliates and/or sub-contractors that Process Personal Data under the instructions or supervision of the Processor but that do not fall under the direct authority of the Processor, such affiliates and/or subcontractors are qualified as Sub-Processor.
Sensitive Data	any set of Personal Data that qualifies as either Criminal Data or as Special Categories of Personal Data.
Special Categories of Personal Data	any set of Personal Data revealing an individual's racial or ethnic origin, political opinions or membership in political parties, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, or social security numbers issued by the government.
Third party	any person, private organization or government body outside Signify.

Transfer of Personal Data	the disclosure of Personal Data by a Group Company to another Group Company, or by these to a Third Party.

Interpretations

INTERPRETATION OF THESE PRIVACY RULES:

(i) Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time

(ii) headings are included for convenience only and are not to be used in construing any provision of these Privacy Rules

(iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning

(iv) the male form shall include the female form

(v) the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa and

(vi) a reference to a document (including, without limitation, a reference to these Privacy Rules) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by these Privacy Rules or that other document, and

(vii) a reference to law includes any regulatory requirement, sectorial recommendation, and best practice issued by relevant national and international supervisory authorities or other bodies.