Signify

Privacy Rules

(Binding Corporate Rules for the transfer of personal data outside the EEA under article 47 GDPR)

Signify confidential

Contact details
Signify Central Privacy Office
privacy.lighting@signify.com

The Edge Amsterdam West, 5th Floor
Basisweg 10
1043 AP Amsterdam
The Netherlands

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	
12 March 2025	Update based upon AP feedback	1.1
12 June 2025	AP approved updated version 1.1	

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") constitute Signify's Binding Corporate Rules for the transfer of Personal Data outside the EEA under article 47 GDPR and 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"), meaning that all Group Companies and employees have to comply with the Signify Privacy Rules, 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.

Capitalized terms have the meaning set out in Annex 1 (Definitions). Capitalized terms that are not defined in these Privacy Rules have the meanings given to them in the GDPR.

Article 1. Scope and Applicability

Scope	**1.1**	These Privacy Rules apply to all Group Companies that act as a Controller or an Internal Processor 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) (or were subject to such data transfer restrictions prior to their transfer to a Group Company outside the EEA), 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**	Personal Data are transferred and/or processed for business purposes set out in Annex 2.
Relation between these Privacy Rules and Applicable Local 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. Each Data Importer shall monitor its local laws and practices and, if it becomes aware that it cannot comply with these Rules (e.g., because it is or has become subject to laws or practices (including Disclosure Requests) that prevent it from complying with these Rules or that have a substantial effect on the protection offered by these Privacy Rules (including on any Data Protection Impact Assessments or Transfer Impact Assessments performed thereunder)), the relevant Data Importer shall promptly notify the relevant Data Exporter and Signify Netherlands B.V. The relevant Data Exporter and Signify Netherlands B.V. shall, following a verification of such notification, determine (in consultation with Signify Group Legal and the Chief Privacy Officer) how to comply with these Privacy Rules and address the conflict, including by implementing appropriate supplementary measures in accordance with Article 3.4. The same applies if the Data Exporter has reasons to believe that the Data Importer can no longer fulfil its obligations under these Privacy Rules. Laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to protect one of the objectives listed in article 23(1) of the GDPR, are not considered to prevent Signify from complying with these Rules or to have a substantial effect on the protection offered by these Privacy Rules. The Data Exporter will monitor, on an ongoing basis, and where appropriate in collaboration with the Data Importer, developments in the Destination Country that could affect the initial Transfer Impact Assessment performed under Article 3.4.
Consequences of Termination of a Transfer	**1.4**	The Data Importer shall – at the Data Exporter's choice – immediately return or delete Personal Data that were received under these Privacy Rules (including any copies thereof), and certify to the Data Exporter that it has done so, where: (i) the transfer has been suspended in accordance with Article 3.4 for a period longer than one month, (ii) the Data Importer is in substantial or persistent breach of these Privacy Rules, (iii) the

		Data Importer fails to comply with a binding decision of a Competent SA or court, or (iv) the Data Importer ceases to be bound by these Privacy Rules. If local laws applicable to the Data Importer prevent the return or deletion of Personal Data, the Data Importer will only process the Personal Data to the extent and for as long as required under that local law. Until the Personal Data are deleted or returned, the Data Importer will continue to ensure a level of protection no lower than that provided for in the Privacy Rules.
Disclosure Requests	**1.5**	Subject to the following paragraph, the Data Importer shall promptly inform the Individual where possible (if necessary, with the help of the Data Exporter) and the Data Exporter, if it receives a Disclosure Request (including if it becomes aware of any direct access to Personal Data transferred under these Privacy Rules by a public authority in the Destination Country). Notifications of a Disclosure Request shall include information about the Personal Data requested, the requesting body, the legal basis for the request and the provided response. In case of direct access to Personal Data by a public authority in the Destination Country, the notification will include all information available to the Data Importer. The Data Importer will assess the legality of a Disclosure Request, in particular whether it remains within the powers granted to the requesting authority. The Data Importer will challenge Disclosure Requests that it, after careful assessment, considers unlawful under the laws of the Destination Country, applicable obligations under international law, or principles of international comity, and under the same conditions shall pursue possibilities to appeal. When challenging a Disclosure Request, the Data Importer shall seek interim measures with a view to suspending the effects of the Disclosure Request until the competent judicial authority has decided on its merits. The Data Importer shall not disclose the Personal Data requested until required to do so under the applicable procedural rules and will only provide the Personal Data that are strictly necessary when complying with a Disclosure Request, based on a reasonable interpretation thereof. The Data Importer will document this assessment and any challenge to the request and provide it to the Data Exporter and, upon request, to any Competent SA 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, the Data Importer will inform the Data Exporter to the maximum extent permitted by applicable law, and will use its best efforts to request the relevant authority to waive this prohibition with a view to communicate as much information as possible and as

soon as possible, will document these efforts, and demonstrate them upon request to the Data Exporter.

The Data Importer will at regular intervals provide the Data Exporter with as much relevant information as possible on the requests received (such as the number of requests, type of Personal Data requested, requesting authority, whether requests have been challenged and the outcome of such challenges). This information will be preserved and provided to any Competent SA upon request. If Data Importer is or becomes partially or completely prohibited from providing such information to the Data Exporter, it will (without undue delay) inform the Data Exporter of such a prohibition.

The Data Importer will provide the minimum amount of information permissible when responding to a Disclosure Request. In any event, any disclosures by Data Importer 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.

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) only if the additional purpose is compatible with the business purpose(s), taking into account the link between the original and additional purpose, the context in which the Personal Data is collected, the nature of the relevant Personal Data and the implementation of appropriate safeguards set out below (**Secondary Purpose**). To the extent not already covered in Article 1.2, and subject to the compatibility assessment referred to above, below are a number of examples of Processing for Secondary Purposes that may be permissible: • 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 limiting access to the Personal Data or taking additional security measures, including encryption or pseudonymization.
Data minimization	**2.5**	Signify shall limit the Processing of Personal Data to those Personal Data that are adequate, relevant and limited to what is necessary for the applicable 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. When the applicable retention period has ended, Personal Data shall promptly be anonymized or destroyed.
Sensitive Data	**2.8**	Signify will only Process Criminal Data where the Processing is authorized by EEA law which provides for appropriate safeguards for the rights and freedoms of Individuals, 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 EEA law (e.g., for reasons of public interest, and for archiving, scientific or historical research purposes or statistical purposes); 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; or
e) Signify has obtained the Individual's explicit Consent.

Privacy rights of Individuals (including complaint handling process)

2.9 According to these Privacy Rules, the Individual has the following rights:

a) Right to obtain a copy of these Privacy Rules (upon request);
b) Right to access, which includes the right to:
    i. 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;
    ii. access to the information listed in Article 3.1 about his/her Personal Data;
    iii. 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;
c) Right to rectification:
    i. the right to have his or her Personal Data rectified without undue delay, if such Personal Data are incorrect or inaccurate;
    ii. taking into account the purposes of the processing, the right to have incomplete Personal Data completed;
d) Right to erasure: the right to have his or her Personal Data anonymized or erased without undue delay if such Personal Data is not Processed in compliance with EEA Data Protection Law or these Privacy Rules, or erasure

is required by EEA law. Signify shall take commercially reasonable steps to inform third parties that are Processing the relevant Personal Data or linking to the relevant Personal Data, that the Individual has requested the erasure of Personal Data by such third parties;

e) Right to restriction: the right to have the Processing of his or her Personal Data restricted from other Processing than storage, pending verification in case the accuracy of such Personal Data is contested or if the Individual objects to such Processing under Article 2.9(f)(i), or where Processing is unlawful or no longer needed, but the Individual prefers restriction to erasure of the Personal Data. Signify will only Process the restricted Personal Data with the Individual's Consent or as permitted by EEA Data Protection Law. Signify will inform the Individual before the restriction is lifted;
f) The right to 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;
    iii. 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;
g) The right to complain: the right to 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;
h) The right to make use of his or her third party beneficiary rights and/or claim damages as described in Article 5.1;
i) The right not to be subject to automated decision-making as described in Article 3.6; and
j) The right to data portability: the right to receive the Personal Data concerning him or her, which he or she has provided, in a structured, commonly used and machine-readable format and have the right to transmit that Personal Data to another controller without hindrance, provided the Processing is done by automated means and based on consent or performance of a contract.

Signify shall communicate any rectification, erasure, or restriction in accordance with the rights in sub (c)-(e) above, to any third party to whom the relevant Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. Signify will inform the Individual about those recipients upon request.

The Individual's right to erasure does not apply in one or more of the following circumstances:

i. the Processing is necessary for compliance with a legal obligation of Signify; or
ii. the Processing is necessary for a task carried out in the public interest, including in the area of public health; or
iii. the Processing is necessary for archiving, scientific or historical research or statistical purposes; or
iv. the Processing is necessary for exercising the right of freedom of expression and information; or
v. the Processing is necessary for the establishment, exercise or defence of a legal claim.

The Individual can exercise the above rights by sending a written request (including by e-mail) to the contact person or contact point indicated by Signify in the relevant privacy notice or by contacting the Privacy Office via the contact details provided at the top of these Privacy Rules.

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

1. show proof of his or her identity when Signify has reasonable doubts concerning such identity, or to provide additional information enabling his or her identification; and
2. 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, Signify's Privacy Office will inform the Individual in writing either:

I. of Signify's position with regard to the request or complaint and any action it has taken or will take in response; or
II. the ultimate date on which the Individual will be informed of Signify's position, which date shall – taking

into account the complexity and number of requests – be no later than two months thereafter.

Signify may, depending on the right, deny the request of the Individual only in the following cases:

All requests:

A. the request does not meet the requirements of this Article;
B. if Signify Processes a large quantity of Personal Data and the request is not sufficiently specific (and the Individual has been given an opportunity to specify their request); or
C. the identity of the Individual cannot be established by reasonable means, including additional information provided by the Individual; or
D. the request is manifestly unfounded or excessive (for example because it constitutes an abuse or rights or because of its repetitive character);
E. in case a specific restriction of the rights of Individuals applies under applicable EEA law;

Requests for erasure:

F. The Processing is necessary for compliance with EEA law;
G. The Processing is required by or allowed for a task carried out in the public interest, including in the area of public health and for archiving, scientific or historical research or statistical purposes;
H. The Processing is necessary for exercising the right of freedom of expression and information;

Requests for erasure and to opt out (right to object):

I. For dispute resolution purposes;

Requests for access and data portability:

J. The request adversely affects the rights and freedoms of Signify or other individuals;

Requests for data portability and to opt out (right to object):

K. The Processing is necessary for the performance of a task carried out in the public interest.

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.

Complaints

The central Privacy Office shall be responsible for complaint handling. Each complaint will be assigned to an appropriate staff member. The relevant staff member shall:

(a) promptly acknowledge receipt of the complaint;
(b) analyse the complaint and, if needed, initiate an investigation; and
(c) when necessary, advise the business on the appropriate measures for compliance and monitor, through to completion, the steps designed to achieve compliance.

Signify will use reasonable efforts to resolve complaints without undue delay, so that a response is given to the Individual within one calendar month of the date that the complaint was filed. Signify shall inform the Individual in writing via the means that the Individual originally used to contact Signify (e.g. via mail or email) either (a) of Signify's position with regard to the complaint and any action Signify has taken or will take in response or (b) when he or she will be informed of Signify's position, which date will be no later than two calendar months after the original one month period. The appropriate staff member shall send a copy of the complaint and his or her written reply to the relevant Privacy Officer.

An Individual may file a complaint with the Chief Privacy Officer:

(d) if the resolution of the complaint by the staff member is unsatisfactory to the Individual (e.g., the complaint is rejected);
(e) if the Individual has not received a response as required by the previous paragraph; or
(f) if the time period provided to the Individual pursuant to the previous paragraph is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he or she will receive a response.

The procedure described in this "*Complaints*" section will apply to complaints filed with the Chief Privacy Officer. An Individual may at all times file a complaint or claim with the

Supervisory Authority or competent court in accordance with Article 5.1, including if the handling of the complaint by the Chief Privacy Officer is not satisfactory to the Individual.

Security and confidentiality

2.10 *Security measures for the protection of Personal Data*

Signify shall protect Personal Data against misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access, using appropriate technical, physical and/or organizational measures, taking into account the state of the art, the cost of their 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.

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

Data Security Breaches are reported without undue delay to the central Privacy Office in accordance with Signify's established incident response procedures, as well as to Signify Netherlands B.V. Where the Group Company that becomes aware of a Data Security Breach acts as a processor in relation to the affected Personal Data, it shall also report the Data Security Breach to the Group Company that is the controller of the Personal Data without undue delay. 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 Supervisory Authority upon request.

In addition, Signify will notify any Data Security Breaches:

- to the Competent Supervisory 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 and, where applicable, the Data Protection Officer;
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, including the identification of the countries, and, in case the transfer is based on a derogation, documentation of suitable safeguards;
f) where possible, the envisaged time limits for erasure of the different categories of Personal Data; and
g) where possible, a general description of the technical and organizational security measures referred to in this Article 2.10.

Where a Group Company is an internal Processor, it shall maintain a record of Processing activities carried out on behalf of the Group Company that is a Controller. This record shall contain information about:

1. the identity of the Controller and the Processor, and, where applicable, the Data Protection Officer;
2. the categories of Processing carried out on behalf of the Controller;
3. where applicable, transfers of Personal Data to non-EEA countries, including the identification of the countries, and, in case the transfer is based on a derogation, documentation of suitable safeguards; and
4. where possible, a general description of the technical and organizational security measures referred to in Article 2.10.

This record shall be maintained in writing, including in electronic form. A copy of this record will be provided to the Competent Supervisory 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 Individuals, the Competent SA 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 Signify shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing of Personal Data 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, or prior to the Processing Personal Data for a Secondary Purpose, 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 country; 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, 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 Supervisory Authority;
- the existence of automated decision making referred to in Article 3.6 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.

Where Personal Data has not been obtained directly from the Individual, Signify shall provide the Individual with the information above:

(a) within reasonable period after obtaining Personal Data but at the latest within one month, having regard to specific circumstances of the Personal Data Processed;
(b) if Personal Data is used for communication with the Individual, at the latest at the time of the first communication with the Individual;
(c) if a disclosure to another recipient is envisaged, at the latest when Personal Data is first disclosed.

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

1. the Individual already has the information referenced above about the intended Processing;
2. 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 outside the EEA, unless the Third Party Processor is required to do so by EEA law 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 the same privacy protection-related obligations 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 onward to a Third Party that is located outside the EEA and not covered by an Adequacy Decision:

a) in accordance with a data transfer mechanism that is recognized under EEA Data Protection Law; or
b) only if a) is not available, if the transfer is subject to a derogation for specific situations under EEA Data Protection Law (i.e., the Processing is necessary for the conclusion or performance of a contract with or in the interest of the Individual (including the implementation of pre-contractual measures taken at the Individual's request), to protect a vital interest of an individual, for the establishment, exercise, or defence of a legal claim, or for important reasons of public interest (as recognized by the EEA law to which the Data Exporter is subject), or the Individual has given his or her explicit consent to the transfer).

Transfer Impact Assessments

3.4 The Signify Group Company that intends to transfer Personal Data under these Privacy Rules will perform a Transfer Impact Assessment prior to a transfer of Personal Data under these Privacy Rules and maintain it for the duration of the transfer.

Where a Transfer Impact Assessment shows gap(s) in protection for Individuals under these Privacy Rules, Signify will implement supplementary measures, such as contractual, technical, or organizational safeguards, including measures applied during transmission and to the Processing of Personal Data in the country of destination to ensure compliance with the Privacy Rules. Supplementary measures are not required in relation to laws and practices applicable to the Data Importer that respect the essence of fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in article 23(1) GDPR.

Transfers shall not take place or will be suspended where: (i) compliance with these Privacy Rules cannot be assured, (ii) no appropriate supplementary measures can be taken, or (iii) so instructed by any Competent SA.

Signify will conduct and document the Transfer Impact Assessment with the involvement of Signify Netherlands B.V. and the Signify Central Privacy Office, and will notify the relevant Data Exporter(s) and Data Importer(s) thereof. Signify Netherlands B.V. and the Signify Central Privacy Office will make the Transfer Impact Assessment, including any applicable supplementary measures, available to all Group Companies, so that the same supplementary measures are applied to the same types of transfers, and to any Competent SA upon request.

Phase 3 – Use of Personal Data

Direct marketing	**3.5**	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 decision making	**3.6**	Individuals have the right not to be subject to a decision which produces legal (or similar significant) effects on them. This restriction does not apply if: a) the use of automated tools is authorized by EEA law in accordance with the requirements of EEA Data Protection Law; b) the decision is necessary for purposes of (a) entering into or performing a contract between the Individual and Signify, or (b) managing the employment-at-will relationship between an Employee and Signify, provided the underlying request leading to a decision by Signify was made by the Employee; or c) the Individual has given his or her explicit consent.

		In the cases referred to in Article 3.6 (b) and (c), Signify shall take suitable measures to safeguard the legitimate interests of the Individual, including at least the right for the Individual to obtain human intervention and to express his or her point of view.
Restrictions under EEA Law	**3.7**	Certain rights of Individuals, Employees and obligations of Signify in these Privacy Rules may in specific cases be subject to restrictions provided by EEA Law, as specified and applied in accordance with EEA Data Protection Law, such as to: a) prevent or investigate criminal offences (including cooperating with law enforcement); b) enforce civil law claims; or c) protect or defend the rights and freedoms of Individuals or the rights or freedoms of others.

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, ensuring 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 Supervisory 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 Supervisory Authorities; and
(viii) manage, oversee and facilitate Signify central Privacy Office (Central Signify Privacy Team) and Privacy Network (Global Signify Privacy Team)

The Chief Privacy Officer annually reports on global data protection risks and compliance issues to the highest level of management of Signify. The Chief Privacy Officer shall enjoy the support of the highest level of management of Signify to perform its tasks.

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 all aspects of the Privacy Rules by Signify is subject to regular review, Signify will (through its Internal Audit function), at least bi-annually as part of its audit program or at the request of the central Privacy Office, perform an audit 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 Privacy Office may request to have an audit as specified in this Article conducted by an external auditor. Applicable professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. 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 and, where appropriate, of Signify N.V. A copy of the audit results related to compliance with the Privacy Rules will be made available, upon request, to the Competent Supervisory Authority.
Training on the Privacy Rules	**4.5**	Signify will, at least bi-annually, provide up-to-date 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 Supervisory 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, investigations or inquiries by Competent Supervisory 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 Supervisory Authority has the authority to audit or inspect (including where necessary on-site) the facilities used by Signify for the Processing of Personal Data for compliance with these Privacy Rules. c) (i) provide to the Competent SA, upon request, information in relation to the Processing of Personal Data subject to these Privacy Rules, and (ii) take into account the advice and abide by binding decisions of the Competent Supervisory Authority on any issue related to these Privacy Rules. Any dispute related to the Competent SA's exercise of supervision of compliance with these Privacy Rules will be resolved by the courts of the Member State of that SA, in accordance with that Member State's procedural law, and Signify Group Companies agree to submit themselves to the jurisdiction of these courts.

Article 5. Final provisions

Third party beneficiary rights and liability	**5.1**	If Signify violates these Privacy Rules with respect to its Processing of an Individual's Personal Data, such Individuals are entitled to enforce compliance with any of the following provisions of these Privacy Rules as third party beneficiaries: (i) Data protection principles (Articles 2.1 – 2.8, 2.10 and 2.11);

(ii) Transparency and easy access to these Privacy Rules (Articles 2.9 (a), 3.1 and 5.4)
(iii) Rights of information, access, rectification, erasure, restriction, objection to processing, right not to be subject to decisions based solely on automated Processing, including profiling (Article 2.9, 3.1 and 3.6);
(iv) Obligations in case of local laws and practices affecting compliance with these Privacy Rules and in case of Disclosure Requests (Articles 1.3 – 1.5 and 3.4);
(v) Right to complain through the internal complaint mechanism of Signify (Article 2.9);
(vi) Cooperation duties with Competent Supervisory Authorities (Article 4.6);
(vii) Liability and jurisdiction provisions, including the rights to judicial remedies, redress and compensation (Article 5.1);
(viii) Duty to inform of updates to these Privacy Rules and to the Group Companies (Article 5.2).

To exercise the rights in respect of these provisions, Individuals are encouraged, but not required to, 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 Supervisory Authority or the courts in the Netherlands, against Signify Netherlands B.V.;
b) the Supervisory Authority in the EEA country where (i) the Individual has his or her habitual residence or place of work, or (ii) the alleged infringement took place, against the Group Company being the Controller or Internal Processor of the relevant Personal Data or against Signify Netherlands B.V.; 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 or the Internal Processor of the relevant Personal Data has an establishment, against such Group Company or against Signify Netherlands B.V.

Liability

Signify Netherlands B.V. accepts liability for a breach of these Privacy Rules by a Group Company located outside the EEA, for which Signify may assert any defense that the relevant non-EEA Group Company could have asserted.

		Individuals may be represented by a not-for-profit body, organization, or association under the conditions set out in EEA Data Protection Laws. 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. The burden of proof is on Signify to prove that it is not liable for any violation of these Privacy Rules which results in a claim for damages by the Individual. 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 Central Privacy Office will maintain a list of all changes/updates to the Privacy Rules since the Privacy Rules came into force, and provide the necessary information to Individuals or Competent Supervisory Authorities upon request. Changes to the Privacy Rules or to the list of Group Companies (if any) will be reported by the Signify Central Privacy Office to the relevant SAs, via the Lead SA, on a yearly basis with a brief explanation of the reasons justifying the update. Where a modification would possibly affect the level of protection offered by these Privacy Rules or significantly affect these Privacy Rules, Signify will communicate this in advance to the relevant SAs, via the Lead SA, including a brief explanation of the reasons justifying the modification.
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 (by publishing these Privacy Rules on a Signify website and on the internal intranet, and providing a copy to individuals upon request in accordance with Article 2.9 (a)). 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**	No Personal Data will be transferred under these Privacy Rules until (1) a 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. Such divested entity shall return or delete all Personal Data received under these Privacy Rules, unless the divested entity can demonstrate that it will continue to apply appropriate safeguards for the protection of such Personal Data in accordance with EEA Data Protection Law (such as by implementing an alternative transfer mechanism). 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.

Annex 1 – 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 one or more specified sectors 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.
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).
Competent SA or Competent Supervisory Authority	The Supervisory Authority competent for the Data Exporter(s) of the specific transfer.
Criminal Data	any Personal Data relating to criminal offenses, criminal records, or proceedings with regard to criminal or unlawful behavior.
Data Exporter	The Group Company that transfers Personal Data under these Privacy Rules.
Data Importer	The Group Company in a Non-Adequate Country that is the recipient of a transfer of Personal Data.
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.
Disclosure Request	a legally binding request for disclosure of (or direct access to) Personal Data from a public authority of a Destination Country.
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 Internal Processor or by a Third Party on behalf of Signify.
Lead SA	Autoriteit Persoonsgegevens, the SA of the Netherlands.
Non-Adequate Country	a country that under EEA Data Protection Laws is deemed not to provide an "adequate" level of data protection.
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.
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.
Signify	Signify Holding Company and Group Companies.
Signify Group Legal	Department responsible for providing legal advice and services to Signify.
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.
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.
Supervisory Authority or SA	the public authority of a country that is responsible for monitoring the application of EEA Data Protection Law within its territory.
Third party	any person, private organization or government body outside Signify.
Transfer Impact Assessment	An assessment on whether, taking into account the specific circumstances of the transfer under these Privacy Rules, the laws and practices of the Non-Adequate Country of destination to which Personal Data are transferred (**Destination Country**), including those requiring the disclosure of Personal Data to public authorities or authorizing access by such authorities, prevent Signify from fulfilling its obligations under these Privacy Rules. Laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in article 23(1) GDPR, are understood not to be in contradiction with these Privacy Rules. In assessing the laws and practices of the Destination Country, Signify shall take into account in particular: (i) the specific circumstances of the transfers, and any envisaged onward transfers within the same Destination Country or to another Destination country, including: • purposes for which data are transferred and Processed (e.g., marketing, HR, storage, IT support); • types of entities involved in the Processing (the Data Importer and any further recipient of any onward transfers); • sector in which the transfers occur; • categories and format of the Personal Data transferred; • location of the Processing including storage; • transmission channels used. (ii) the laws and practices of the Destination Country relevant in light of the circumstances of the transfers, including requirements to disclose Personal Data to public authorities or authorizing access by such authorities as well as the applicable limitations and safeguards. This also includes laws and practices providing for access to Personal Data during transit between the country of the Data Exporter and the Destination Country; (iii) any relevant contractual, technical or organizational safeguards put into place to supplement the safeguards under these Privacy

Rules, including measures applied during transmission and to the Processing of Personal Data in the Destination Country.

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.

Annex 2 – Description of Processing of Personal Data

The tables below describe the categories of Personal Data, the types of Processing activities, the Processing Purposes and the categories of data subjects whose Personal Data are Processed under these Privacy Rules. As a global group of companies, Signify continuously transfers Personal Data between its various Group Companies for the purposes set out in below. A list of the Group Companies, including the countries where they are located, is available here.

1. Categories of Personal Data

Category of Personal Data	**Examples of Personal Data Elements**
Personal Data of consumers, business customers, suppliers, business partners and other natural persons (such as research participants) only:	
Personal identification data	Name, surname, title, date of birth
Contact information data	Email, phone number, address, country
Account log in information	Log in ID, password or other security codes
Device information	Hardware model, and other unique device identifiers, app installation identifiers, IP address, operating system version
Signify device information	Hardware model, Device physical IDs, and other unique device identifiers, device MAC address, IP address, operating system version, device settings used to access the services, and device configuration
Log information	Time, duration and manner of use of Signify products and services or products and services connected to Signify
Location information	Location (derived from IP address, Bluetooth beacons or identifiers, or other location-based technologies), that may be collected when enabling location-based products or features such as through Signify apps
Images, quotes and/or videos from which an Individual may be identified	Pictures uploaded to Signify accounts or otherwise provided to Signify, for example, in the context of a webinar or interview
Financial data	Credit card data, bank account data
Other information about Individuals' use of Signify digital channels or products	Apps or websites that Individuals use or visit, links that Individuals click within Signify advertising e-mail, analytic data via cookies and similar technologies,
Any other information that Individuals decide to voluntarily share with Signify or its affiliates	Feedback, opinions, reviews, comments, uploaded files, interests, information provided for our due diligence process

Personal Data of job applicants or Employees only:	
Basic personal details	Name, organization, Employee identification number, work contact details (email, phone numbers, physical office address)
Other personal details	Home contact details (email, phone numbers, physical address), language(s) spoken, age, gender, date of birth, national identification number, region, internal identification number, social security number, marital/civil partnership status, domestic partners, dependents, emergency contact information
Documentation required under immigration laws	Citizenship, passport data, details of residency or work permit, visa
Relationship details	Term of employment and/or termination date and reasons, work history (current and former employers), hire/re-hire, position as a (former) member of the board, and position of (former) shareholders
Compensation and payroll	Base salary, bonus, benefits, details on stock appreciation rights and other awards, compensation type, currency, pay frequency, effective date of current compensation, salary reviews, banking details
Performance data	Performance and development reviews; information for talent development programs and diversity programs, details on performance management ratings, planned or attended development programs
Position information	Description of current position, job title, company name (legal employer entity), branch/unit/department, location, employment status and type, full-time/part-time, terms of employment, employment contract, length of service, retirement eligibility, promotions, and disciplinary records
Recruitment information	Details contained in letters of application and resume/CV (previous employment background, education history, professional qualifications, language and other relevant skills, certification, certification expiration dates), application status
Operational information	Working time records (including vacation and other absence records, leave status) staffing information, onboarding and offboarding information, relocation services, security information, information relating to internal investigations, risk-management information, health, and safety information.
System and application access data	Authentication information, information required to access company systems and applications such as user and system IDs for company network or servers, email account, and passwords.
Network traffic and other related data	Identification numbers, location data, online identifiers, IP address, cookies, device ID, Websites visited, language settings, and voice data.
Racial or ethnic data	Photos (e.g. a copy of a passport containing a photo) and video images which, in some countries, qualify as racial or ethnic data, diversity and inclusion information
Physical or mental health data	Any information on physical or mental health and data relating to disabilities, disability status, and absence due to illness or pregnancy
Criminal data	Information relating to criminal behavior, criminal records or

	proceedings regarding criminal or unlawful behavior
Religious or philosophical beliefs	Information on religious or philosophical beliefs, church affiliation
Trade union membership	Information of trade union membership of Employee
Biometric data	Data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person

2. Purposes for which Personal Data is Processed

Purpose of Processing	Examples of Processing Activities
Assistance of a customer, consumer, supplier, business partner, job applicants or Employees	This purpose includes the Processing of Personal Data in connection with providing personalized support, upon request (e.g. customer service or 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, management of company and employee 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, performing internal surveys, implementing business controls, management reporting and analysis, managing and using employee directories, managing courses and/or trainings, managing projects and costs, management of alliances, ventures, mergers, acquisitions and/or divestitures, re-organizations or disposals and integration with purchaser, management reporting and analysis, archive and insurance purposes, legal or business consulting, budgeting, financial and reporting, communications, government and legal affairs, intellectual property management
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, its Employees in the sector in which it operates 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 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, 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 job applicants, Employees, 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
Personal Data of consumers, business customers, suppliers, business partners and other natural persons (such as research participants) only:	
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
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, enrichment of Signify personal data from Signify-owned data sources, 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
Personal Data of job applicants or Employees only:	
Assessment and acceptance of job	This purpose includes the Processing of Personal Data in connection with recruitment activities, such as the evaluation of

applicants	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)
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)
Employee communications (incl. direct marketing)	This purpose includes the Processing of Personal Data in connection with activities such as communications around specific employee discounts, social media-related activities, raffles and giveaways such as brand ambassador programs, or invitations for charity initiatives and other events

3. Purposes for which Sensitive Data are Processed

Purpose of Processing	**Examples of Processing Activities**
Security and facility access	In some countries photos and video images of Individuals qualify as racial or ethnic data. Signify may process photos (e.g. a copy of a passport containing a photo) and video images for the protection of (the interests and assets of) Signify and its Employees, joint ventures, participations, clients, supplier and business partners (including safeguarding the integrity of Signify, pre- and in-employment screening of Employees and monitoring of Employees), to record decisions made in the course of business for future reference (e.g. when Individuals participate in video conferencing which is recorded), for site access and security reasons, demographic reporting under applicable anti-discrimination laws, for obtaining visa's, permits and technology export licenses and for inclusion in Employee directories
Preferential status based on ethnicity or culture	This purpose includes providing preferential status to persons from particular ethnic or cultural minorities to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant Sensitive Data allows for an objective determination that an individual belongs to a minority group and the Individual has not filed a written objection against the relevant Processing
D&I and ESG reporting	Monitoring and reporting on Signify's D&I efforts and complying with ESG reporting requirements under applicable law
Administering Affinity Groups	Administering Employee affinity groups

Purpose of Processing	Examples of Processing Activities
Health services	Providing health services to an Employee provided that the relevant health data is processed by or under the supervision of a health professional who is subject to professional confidentiality requirements
Administering pensions and benefits	Administering pensions, health and welfare benefit plans, maternity, paternity or family leave programmes, or collective agreements (or similar arrangements) that create rights depending on the state of health of the Employee
Preferential status based on health status	Providing preferential status to persons with a particular disability to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant Sensitive Data allows for an objective determination that an Employee belongs to the relevant category and the Employee has not filed a written objection against the relevant Processing
Re-integration and support	Reintegrating or providing support for Employees entitled to benefits in connection with illness or work incapacity
Pre- and in-employment screening	Pre- and in-employment screening and monitoring of Employees and for assessing and making decisions on (continued) eligibility for positions, projects or scope of responsibilities
Facility management	Providing facilities in the workplace to accommodate health problems or disabilities
Background checks	Assessing an application by an Employee to make a decision about the Employee or provide a service to the Employee
Screening for criminal activities	Protecting the interests of Signify, its Employees, customers, suppliers and business partners with respect to criminal offences that have been or, given the relevant circumstances are suspected to be or have been, committed against Signify, its Employees, customers, suppliers and business partners, and further for pre- and in-employment screening and monitoring of Employees
Administering Employee pensions, benefits, and memberships	Processing data on sexual preference (including data relating to partners of Employees) for the purpose of administering Employee pensions, benefits programs, and memberships
Accommodating religious or philosophical practices	Processing data on religious or philosophical beliefs insofar as necessary for accommodating religious or philosophical practices, dietary requirements or religious holidays
Biometric security	Biometric security and access management purposes in relation to Signify's premises, systems and assets
Trade union membership payment	Payment of the membership of trade union of the Employee