



## SIGNIFY

### **Privacy Notice for the Recruitment Process**

Latest update: June 2023

#### INTRODUCTION

Your privacy is important to Signify.

We have drafted this Privacy Notice (also referred to as "Notice") in order to help you understand who we are, what Personal Data we collect about you, why we collect it, and what we do with it during our recruitment process. When we talk about "Personal Data" (in this Notice also referred to as "Data" or "your Data") we mean any information or set of information from which we are able, directly or indirectly, to personally identify you, in particular by reference to an identifier, e.g. name and surname, email address, phone number, etc. Signify protects Personal Data of individuals (e.g., consumers, business customers, employees, job applicants, and other natural persons) in line with its Signify Privacy Rules ("Privacy Rules", also referred to as "BCRs") which can be found [here](#).

Because Signify is an international company, this Notice may be replaced or supplemented in certain regions to fulfil local requirements and to provide you with additional information.

We advise you to take some time to read this Notice. If you do not agree with the processing described in this privacy notice, please do not provide your data to us. Please note that your choice not to provide any of your Data as required or requested in the context of the recruitment procedure, may have effect on your ability to participate in the recruitment process. Any information you share with us as part of your application procedure must be true, complete and not misleading to avoid the risk of a rejection of your application during the application process or disciplinary action, including immediate termination, during employment.

#### WHEN DOES THIS PRIVACY NOTICE APPLY?

This Notice covers how we collect and use your Data in the context of our recruitment process. For example, when you apply for a job offered by, use our recruitment channels, visit our career websites, create a profile, join our recruitment events, join our talent community, when we contact you for job opportunities or when you otherwise interact with us in your capacity as candidate or job applicant.

By engaging in our recruitment process (where legally required), including organizing the selection process and applications, you expressly consent to our collection, storage, use, transfer, and disclosure of your Data, including any sensitive information you elect to submit (as described in this Privacy Notice).

#### WHO IS SIGNIFY?

Signify is the world leader in lighting. We provide professional customers and consumers with quality, energy-efficient LED lighting. Our lights, when connected, bring data to devices, apps and people, redefining what light can do and how you use it. Today, our innovations, such as LiFi, internet connectivity through light, and UV-C, solar and horticultural lighting, contribute to a safer, smarter and more sustainable world.

When this Notice mentions "we", "us", or the "Company", it refers to Signify Netherlands B.V. (Registration number 17061150 - High Tech Campus 48, 5656 AE, Eindhoven, The Netherlands) as well as the Signify Affiliate(s) which may be interested in offering you a position or that otherwise decides which of your Data are collected and how they are used. Please note that the Signify Affiliates include the subsidiary companies in which Signify N.V. has control, either through direct or indirect ownership. You may obtain a list of the Signify's Affiliates by contacting the Signify Privacy Office (you will find the contact details in the below section "What are Your Privacy Rights?").

#### WHAT TYPES OF PERSONAL DATA DO WE COLLECT ABOUT YOU?

Below you will find an overview of the categories of Data that we may process during the recruitment process, information you provide to us directly.

Categories of Personal Data	Examples of types of Personal Data We Collect
Personal identification data	Name, surname, title, gender, country, date and place of birth, military status (only in certain countries), nationality, language(s) spoken, marital/civil partnership status, domestic partners, dependents.
Contact information data	Email, phone, address
Network traffic data and other related data	Identification numbers, location data, online identifiers, IP address, cookies, device ID, websites visited, language settings.
Account login information	Login ID, password, other information used to access and/or secure Company systems and applications including the career website
Images and/or videos from which you may be identified	Pictures uploaded into CV, candidate profile or otherwise provided by you to us. Videos recorded during the optional video interview. Images or other Data captured by cameras and sensors when physically present on our premises and/or office locations.
Data regarding qualifications and career development	Any information contained in CVs and additional documents containing personal details (e.g. diplomas, certificates) as provided by applicants or any information, following from CVs or additionally, submitted by applicants as part of the application (for example confirmation(s) of employment history, relevant experience, academic achievements and GPA's (for US interns only), assessment and/or test evaluation information, evaluations of interviews conducted with applicants, educational and employment background, job qualifications, jobs for which the applicant would like to submit an application, willingness to relocate, driver's license information, any additional information such as transcripts, employment references and related information, compensation requests.
Information resulting from background or employment check and/or an employment reference	Feedback, opinions
Special categories of Personal Data	When permitted by local law: <ul style="list-style-type: none"> <li data-bbox="576 1749 1458 1850">☐ Information about disabilities to the extent relevant for the performance of your work: for instance, where we would be required to make work or workspace adaptations, accommodations, or adjustments.</li> <li data-bbox="576 1850 1458 1957">☐ Racial or ethnic data: for instance, where this would show from pictures, photographs, and other visual images, but also where such data is processed for diversity related purposes.</li> </ul>

## Categories of Personal Data

## Examples of types of Personal Data We Collect

*Note: We generally process these special categories of data in order to comply with legal obligations and internal policies, such as relating to diversity and anti-discrimination.*

### Criminal data

Data relating to criminal behaviour, criminal records or proceedings regarding criminal or unlawful behaviour (only in certain countries, for certain roles and only upon request of Signify).

### Compensation and payroll

Bank account information (to support expenses of certain applicants), desired salary, compensation, and benefits.

### Any other information that you decide to voluntarily share with Signify

Feedback, areas of interest, opinions, information provided in emails and letters, during telephone calls and conversations.

**We value diversity and inclusion. In order to ensure equal employment opportunities as permitted or required by local law we may also gather Data of a sensitive nature, including your nationality, racial and/or ethnic origin, gender and disability. Equal employment opportunities mean we offer equal treatment to all applicants. You can choose to provide this information on a voluntarily basis. Where we have a mandatory legal obligation to process aforementioned Data, the relevant job vacancy will indicate if that it is mandatory.**

If you provide us with Personal Data of a reference or any other individual as part of your application, it is your responsibility to obtain consent from that individual prior to providing the information to us. It is your responsibility to ensure that information you submit does not violate any third party's rights.

#### *Information we collect automatically*

When you apply for a job offered by us, join our talent community, use our recruitment channels, or visit our career websites, in addition to the information you provide to us directly, we may collect information sent to us by your computer, mobile phone or other access device. For example:

##### ◦ **Device information**

Such as your hardware model, IMEI number and other unique device identifiers, MAC address, IP address, operating system version, and settings of the device you use to access the Services.

##### ◦ **Log information**

Such as the time and duration of your use of our channel.

##### ◦ **Location information**

For example, a location derived from your IP address or data that indicates where you are located, such as at a city or postal code level.



◦ **Other information**

About your use of our digital channels, such as the apps you use or the websites you visit. For more information on how we use cookies and other tracking technologies, read the Signify Cookie Notice which can be found at the website of the [Signify Privacy Center](#), see “Legal information” section. You can control your cookie settings via the cookie preference choices.

Lastly, if you visit our premises, for security reasons and in line with local requirements we might also record your Data through video or other electronic, digital, or wireless surveillance system or device (e.g., CCTV).



### Information we may collect from other sources

To the extent permitted by applicable law, in addition to our recruitment channels or career websites, we may also obtain information about you from other sources, such as through your interactions with Signify personnel or from third parties, such as recruiters, recruitment agencies, LinkedIn or other websites on the Internet (subject to such third party's privacy notices), or from a background check report. For example, you may choose to provide us with access to certain data stored by third parties such as business and employment-oriented social media sites.

### HOW DO WE USE YOUR PERSONAL DATA?

We may use your Data for the purposes of carrying out your application and the entire recruitment process. Below you will find an overview of the purposes for which we may process your Data during the recruitment process:

Purposes for processing Personal Data	Examples
Assessment and acceptance of job applicant	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).
Job Applicant support (upon your request)	Assistance via talent acquisition teams and other communication channels.
Human Resources and Personnel Management	To contact you by phone call, text (SMS), or email messaging, to inform applicants of available vacancies, to provide with information relating to application and to fulfil applicants' requests, to offer applicants suitable opportunities for employment within Signify.
Job alert subscription (upon your request)	Sharing personalized job opportunities recommendations that match your areas of interest or skills and Signify news in your expressed areas of interest.
Security and protection of interests/assets of Signify or Signify employees	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.
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

Purposes for processing Personal Data	Examples
---------------------------------------	----------

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.

Defence 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.
-------------------------	---

### ON WHAT LEGAL BASIS DO WE USE YOUR DATA?

In order to be able to process your Data, we may rely on different legal bases, including:

- Your consent (only when legally permitted or required). If we rely on your consent as a legal basis for processing your Personal Data, you may withdraw your consent at any time; or
- The necessity to establish a contractual relationship with you; or
- The necessity for us to comply with legal obligations and to establish, exercise, or defend our self from legal claims; or
- The necessity to pursue our legitimate interests, including:
  - to ensure that our networks and information are secure;
  - to administer and generally conduct business within the Company and across Signify;
  - to prevent or investigate suspected or actual violations of law, breaches of the terms of employment or non-compliance with the Signify Integrity code or other Signify policies;
  - the necessity to respond to your requests (such as responding to your requests regarding the handling of, deletion of, or changes to your Personal Data); and
  - to optimize your job opportunity search across Signify and communication relevance.
- The necessity to protect the vital interests of any person; or
- Any other legal basis otherwise permitted by local laws.

If you would like to request more details about our legal bases on which we process your data for a particular purpose, you can contact the Signify Privacy Office (you will find the contact details in the below section “What are Your Privacy Rights?”).

### WHEN DO WE SHARE YOUR PERSONAL DATA?

We do not share any of your Personal Data except in the limited cases described here. To fulfil the purposes for which your Personal Data has been collected (for details on these purposes, see above section “How do we use your personal information?”) we may disclose your Personal Data to the following entities.

1. *Signify Affiliates*: Due to our global nature, your Personal Data may be shared with certain Signify Affiliates. Access to Personal Data within Signify will be limited to those who need to know the information, for the purposes described in this Notice, and may include your interviewers, the relevant manager(s) of the respective job offer and other selected personnel within Signify.
2. *Service Providers*: Like many businesses, we may outsource certain Personal Data processing activities to trusted third party service providers to perform functions and provide services to us, such as:
  - ICT service providers
  - Recruitment- or assessment provider
  - Consulting providers
  - Background check provider
  - Travel-, security- and safety provider



3. *Public and Governmental Authorities.* When required by law, or as necessary to protect our rights, we may share your Personal Data to entities that regulate or have jurisdiction over Signify.
4. *Professional advisors and others.* We may share your Personal Data with other parties including professional advisors, such as:
  - Banks
  - Insurance companies
  - Auditors
  - Lawyers
  - Accountants
  - Other outside professional advisors
5. *Other parties in connection with corporate transactions.* We may also, from time to time, share your Personal Data in the course of corporate transactions, such as during a sale of a business or a part of a business to another company, any reorganization, merger, joint venture, or other disposition of Signify's business, assets, or stock (including in connection with any bankruptcy or similar proceeding).

We will also, upon your request of Personal Data portability, share your Personal Data with the party you indicate.

#### WHEN DO WE TRANSFER YOUR PERSONAL DATA ABROAD?

Due to our global nature, the Personal Data you provide to us may be transferred to or accessed by Signify Affiliates and trusted third parties around the world for purposes described in this Notice. As a result, your Personal Data may be processed outside the country where you live and/or applied for a job.

If you are located in a country member of the European Economic Area, we may transfer your Personal Data to countries located outside of the European Economic Area. Some of these countries are recognized by the European Commission as providing an adequate level of protection, for countries not recognized we have put in place adequate measures to protect your Data, such as organizational and legal measures (e.g., Binding Corporate Rules and approved European Commission standard contractual clauses, or similar frameworks). Whenever Personal Data is transferred outside the country you are located in, for the purposes mentioned above, the local legal requirements will be taken into account and/or above adequate measures will apply in order to protect your data sufficiently. You may request more details, and where applicable obtain a copy, of these measures that we have in place in respect to transfers of Personal Data by contacting the Signify Privacy Office. You will find the contact details in the below section "What are Your Privacy Rights?"

#### HOW LONG DO WE KEEP YOUR PERSONAL DATA?

We keep your Personal Data for the period necessary to fulfil the purposes for which it has been collected (for details on these purposes, see above section "How Do We Use Your Personal Data?") and we may retain and use your Data to consider you for other positions.

The criteria used to determine our retention/conservation periods include:

- How long is the Personal Data needed to provide you with a job offer?
- Do you have an account with us? In this case we will keep the Data while your account is active or for as long as needed to provide services to you.
- Have you indicated that we can retain your Data to consider you for other positions?
- Are we subject to a legal, contractual, or similar obligation to retain the Personal Data? Examples can include mandatory data retention laws in the applicable jurisdiction, government orders to preserve Data relevant to an investigation, or Data that must be retained for the purposes of litigation.

If you have decided to participate in our optional live and/or on demand video interview during the recruitment process, videos of your interview will be retained for 90 days from their creation, after which they will be deleted unless local law requires differently and/or we have overriding company interest (e.g. the necessity for us to comply with legal obligations and to establish, exercise, or defend our self from legal claims or to pursue our legitimate interests).

Your Personal Data processed is used to improve your experience with us, and is retained for as little time as possible, after which we anonymize or delete it, when there is no longer a talent acquisition purpose, legal or business need for your data to be retained.



If you would like to find out how long we keep your data for a particular purpose you can contact the Signify Privacy Office (you will find the contact details in the below section “What are your Privacy Rights?”). Of course, if you do not want to be considered for other positions or would like to have your Data removed, you can contact us via this [link](#), or through your application profile.

### HOW DO WE SECURE YOUR DATA?

To protect your Data, we will take reasonable and appropriate physical, technical and administrative measures that are consistent with applicable privacy and data security laws and regulations. This includes requiring our service providers to use appropriate measures to protect the confidentiality and security of your Personal Data. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. Depending on the state of the art, the costs of the implementation and the nature of the data to be protected, we put in place technical and organizational measures to prevent risks such as destruction, loss, alteration, unauthorized disclosure of, or access to your Data. If you have reason to think that your interaction with us or your Data is no longer processed in a secure manner, please reach out immediately in accordance with “What are Your Privacy Rights?” as described below.

### WHAT ARE YOUR RESPONSIBILITIES?

We would like to remind you that it is your responsibility to ensure, to the best of your knowledge, that the Data you provide to us is accurate, complete, and up to date. Furthermore, if you share Personal Data of other people (such as dependents) with us, it is your responsibility to collect such Data in compliance with local legal requirements. For instance, you should inform other people, whose Personal Data you provide to the Company, about the content of this Notice and obtain their consent (provided they are legally competent to give consent) for the use of that Personal Data by the Company as set out in this Notice (including transfer and disclosure).

### WHAT ARE YOUR PRIVACY RIGHTS?

We aim to provide you with access to your Data. Usually, you can control your Personal Data (e.g., by logging to your account) and update, modify, or, if legally possible, delete it. In any case, we strongly encourage you to take control of your Personal Data. You may exercise certain rights regarding your data processed by us by contacting us via this [link](#) or via [Signify Privacy Center](#) (see “Privacy request section”) . In particular, you have the right to do the following (please take into account that some of these actions will mean you will be removed from the recruitment process):

- **Withdraw your consent at any time.** You have the right to withdraw consent where you have previously given your consent to the processing of your data. Please understand that withdrawal of consent by you will not affect the validity of previous Personal Data processing that was conducted prior to the withdrawal based on your authorization
- **Object to processing.** You have the right to object to the processing of your data if the processing is carried out on a legal basis other than consent or when its solely based on automated processing and produces adverse legal effects. Further details are provided in the dedicated section below.
- **Access.** You have the right to learn if your Data is being processed by us, obtain disclosure regarding certain aspects of the processing and obtain a copy of your data undergoing processing.
- **Verify and seek rectification.** You have the right to verify the accuracy of your data and ask for it to be updated or corrected.
- **Restrict the processing.** You have the right, under certain circumstances, to restrict the processing of your data. In this case, we will not process your data for any purpose other than storing it.
- **Delete.** You have the right, under certain circumstances, to obtain the erasure of your data from us.
- **Receive and transfer to another controller.** You have the right to receive your data in a structured, commonly used and machine-readable format and, if technically feasible, to have it transmitted to another controller without any hindrance. This provision is applicable provided that your data is processed by automated means and that the processing is based on your consent, on a contract which you are part of or on pre-contractual obligations thereof.
- **Lodge a complaint:** you have the right to lodge a complaint with your Regulator/Data Protection Authority. We hope to resolve any queries or concerns, however if you are unsatisfied with the reply received, you may then refer your complaint to the relevant Regulator/Data Protection Authority in your jurisdiction.





For any other questions or your reasonable inquiry related to the protection of your Personal Data by Signify or regarding this Notice in general, you can contact the Signify Privacy Office/Chief Privacy Officer/DPO at:

- Mail: Signify - Attn: Privacy Office - Basisweg 10, 1043 AP Amsterdam, The Netherlands; or
- Online: [Signify Privacy Center](#), "Privacy request" section.

Please keep in mind that email and online communications are not always secure. Therefore, please do not include sensitive information in your emails to us.

We will do our best to address your request in time and free of charge, except where it would require a disproportionate effort. We may ask you to verify your identity before we can act on your request.

#### **BRAZIL PRIVACY DISCLOSURES**

The Brazilian General Law on Data Protection (the "LGPD") provides any person located in Brazil and/or any Personal Data that has been collected or is processed within Brazil with specific rights over their Personal Data. In addition to the above, this section describes your LGPD rights and explains how to exercise those rights.

The following does not apply to information or data that cannot identify you or another person, taking into account the use of reasonable and available technical means at the time of its processing.

#### **INTERNATIONAL TRANSFER OF PERSONAL DATA**

As described above in this Notice, it may be necessary for Signify to transfer your Personal Data internationally.

We may transfer your Personal Data to countries located outside of Brazil. Some of these countries do not have an adequate level of protection for Personal Data, as determined by the General Data Protection Law. If the international transfer of Personal Data occurs to countries that do not have Personal Data protection laws at the same level as the LGPD, we will adopt appropriate measures to protect your Personal Data, such as organizational and legal measures (e.g. binding rules and standard contractual clauses for such transfer).

#### **YOUR PRIVACY RIGHTS**

You have the right to request:

- I. confirmation whether we process (or not) your Personal Data
- II. access to your Personal Data processed by us
- III. rectification of your Personal Data
- IV. portability of your Personal Data
- V. anonymization, blocking or deletion (erasure) of unnecessary or excessive data or data processed in breach of the provisions of the LGPD
- VI. deletion of Personal Data processed based on your Consent, with the exceptions provided for in the LGPD
- VII. the information of the public and private entities with which Signify has carried out shared use of Personal Data
- VIII. information on the possibility of not providing *Consent* and the consequences of refusal
- IX. revocation of Consent, under the terms of the LGPD

In certain circumstances, you have the right to object and restrict the processing of your Personal Data and/or request a review of automated decisions affecting your interests. Our Privacy Notices set out full information on how you can exercise these rights, how we share Personal Data with third parties, how we protect your Personal Data and how we ensure that your data is adequately protected if it is processed outside of Brazil. To contact Signify, please check the "What are your Privacy Rights" section in the Notice above. You also have the right to contact the National Data Protection Authority ("ANPD") directly.

#### **CALIFORNIA PRIVACY DISCLOSURES**

The California Consumer Privacy Act (hereafter: 'CCPA') and the California Privacy Rights Act (hereafter: 'CPRA') provide California consumer residents (including Job Applicants who reside in California, hereafter: 'Job Applicants') with specific rights regarding their personal information. In addition to the above this section describes your CCPA/CPRA rights and explains how to exercise those rights.



The following is not applicable to de-identified or aggregated personal information or data publicly available.

### INFORMATION WE COLLECT

Mindful and respecting the three primary exemptions as defined in AB 25 CCPA, we inform you that when visiting our Career website and/or in the context of our recruitment we collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device (defined as “**Personal Data**”). The purposes for which we collect Personal Data you can find above under “FOR WHICH PURPOSES DO WE USE YOUR DATA?” and information about retention can be found under “HOW LONG DO WE KEEP YOUR *PERSONAL DATA*? In particular, we might collect and/or have collected and disclosed for the aforementioned purpose within the last twelve (12) months prior to the effective date of this Notice the following categories of data from you:

Category	Examples	We Collected	We Disclosed
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver’s license number, passport number, or other similar identifiers.	YES	YES, to affiliates, service providers, and other vendors mentioned in this Notice
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	YES	YES, to affiliates, service providers, and other vendors mentioned in this Notice
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	YES	YES, to affiliates, service providers, and other vendors mentioned in this Notice
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	NO	NO
E. Biometric information.	Genetic, physiological, behavioural, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO	NO
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer’s interaction with a website, application, advertisement or other content.	YES	YES, to affiliates, service providers, and other vendors mentioned in this Notice



G. Geolocation data.	Physical location or movements, or the location of your device or computer.	YES	YES, to affiliates, service providers, and other vendors mentioned in this Notice
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	NO	NO
I. Professional or employment-related information.	Current or past job history or performance evaluations.	YES	YES, to affiliates, service providers, and other vendors mentioned in this Notice
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	YES	YES, to affiliates, service providers, and other vendors mentioned in this Notice
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	YES	YES, to affiliates, service providers, and other vendors mentioned in this Notice
L. Sensitive Personal Information	Personal information that reveals a consumer's social security, driver's license, state identification card, or passport number; account log-in, password, or credentials allowing access to an account; racial or ethnic origin; health. Some personal information included in this category may overlap with other categories.	YES	YES, to affiliates, service providers, and other vendors mentioned in this Notice

We disclose your data for a business purpose to the following categories of third parties:

- Signify Affiliates.
- Service providers.
- Third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.

#### DO NOT SELL?

We do not respond to "Do Not Sell" requests as we do not track your data across third party websites, nor do we sell your data to third parties to provide targeted advertising. Nonetheless, we aim to make your online experience and interaction with our websites as informative, relevant and supportive as possible. One way of achieving this is to use cookies or similar techniques, which store information about your visit to our site on your computer. For more information on how we use cookies and other tracking technologies, read our [Cookie Notice](#). In the twelve months prior to the effective date of this Privacy Notice, we have not sold any personal information of consumers, as those terms are defined under the CCPA.

#### YOUR PRIVACY RIGHTS

"Right to Know": You may have the right to request that we disclose to you what personal information of yours that we collect, use, and/or disclose.

"Right to Delete": You may have the right to request the deletion of your personal information collected or maintained by us. Depending on your Choices, certain offerings may be limited or unavailable. Upon verifying



the validity of a deletion request, we will delete your personal information from our records, and instruct any service providers or third parties to delete your information, when applicable.

“Right to Control Use”: You may have the right to control or limit the use of your personal information, including:

- Right to Opt Out of Sales/Sharing/cross context behavioral advertising
- Right to Object to or Opt Out of automated decision making/profiling
- Right to Opt Out of processing/Limit Use of sensitive Personal Data

“Right of Access”: You may have the right to access your personal information, and to transmit it to another entity.

“Right of Correction”: You may have the right to request amendments to your personal information if it is inaccurate or outdated in any way. Upon verifying the validity of a verifiable correction request, we will use commercially reasonable efforts to correct your personal information as directed, taking into account the nature of the personal information and the purposes of maintaining your personal information.

Please note that the above rights are not absolute, and we may be entitled to refuse requests, wholly or partly, where exceptions under applicable law apply.

### SUBMITTING A QUESTION OR REQUEST TO EXERCISE YOUR RIGHTS

If you have questions about the foregoing or how to execute your rights in our Privacy Notice or specifically with regard to categories and specific data processed, categories of sources from which your data is collected by us, categories of third parties with whom we share your data, and the business and/or commercial purpose for collecting, please contact our Privacy Office (see section “What are your Privacy Rights?”). You may also make a verifiable request to exercise your rights by contacting us via this [link](#).

If we cannot verify your identity (or your authority to act on behalf of another person) we have the right to deny requests. While verifying your identity we shall generally avoid requesting additional information from you for purposes of verification. If, however, we cannot verify your identity from the information already maintained by us, we may request additional information from you, which shall only be used for the purposes of verifying your identity while you are seeking to exercise your rights under the CCPA/CPRA, and for security or fraud-prevention purposes. We shall delete any new personal information collected for the purposes of verification as soon as practical after processing your request, except as required to comply with applicable legislation.

An “authorized agent” means a natural person, or a business entity registered with the Secretary of State that you have authorized to act on your behalf provided you have:

1. Provided the authorized agent written permission to do so and we could verify this; and
2. Verified your own identity directly with the business.

Subsection 1 does not apply when you have provided the authorized agent with a valid power of attorney.

We do utmost to timely respond to a verifiable Individual, free of charge and in a portable format unless it is excessive, repetitive, or materially unfounded. If we require more time, we will inform you of the reason thereof and extension period in writing. If you prefer not to use the provided [link](#) you may also exercise your rights by contacting us via the toll-free telephone 1-800-555-0050.

### NON-DISCRIMINATION

We will not discriminate against you for exercising your rights under the CCPA/CPRA.

Based on the complexity of the request and the applicable regulations, we may charge a fee for your request. We may offer a CCPA/CPRA-permitted financial incentive, participation in a financial incentive program requires your prior opt in Consent, which you may revoke at any time.

### CHINA PRIVACY DISCLOSURES

The Chinese Personal Information Protection Law (the "PIPL") provides any person located in China and/or any Personal Data that has been collected or is processed within China with specific rights and obligations aimed at



protecting the rights and interests of individuals, regulating Personal Data processing activities, and facilitating reasonable use of Personal Data. The following does not apply to information or data that cannot identify you or another person, considering the use of reasonable and available technical means at the time of its processing.

Where conflicting, what is contained in this disclosure will supersede any other provisions contained in this Privacy Notice contrary to or inconsistent with the below. For purpose of this Notice, “China” refers to mainland China, excluding Hong Kong Special Administrative Region (“SAR”), Macau SAR, and Taiwan Region.

#### OUR LEGAL BASIS

We will process your data in accordance with the principles of legality, legitimacy, necessity, and good faith. For situations where the PIPL applies, we will base our processing activities on the following bases:

- Your Consent, which you may withdraw at any time
- Where it is necessary to enter into or perform a contract to which you are a party, or for the implementation of human resources management in accordance with the labour rules and regulations formulated in accordance with applicable laws and the collective contract concluded in accordance with applicable laws
- Where it is necessary for the performance of statutory duties or statutory obligations
- Where it is necessary to respond to a public health emergency, or for the protection of the life, health and property safety of a natural person
- To a reasonable extent, for purposes of carrying out news reporting and media monitoring for public interests
- Where we reasonably process the Personal Data that has been publicly disclosed by you or otherwise disclosed publicly in a lawful manner within a reasonable scope in accordance with the provisions of PIPL
- Other circumstances stipulated by laws and administrative regulations

#### YOUR RIGHTS

In addition to the rights mentioned in the section “WHAT ARE YOUR PRIVACY RIGHTS?”, for situations where the PIPL applies, you also have the right to request us to explain decisions that have significant impact on your rights and interests and are made through automated decision-making technologies, and to refuse decisions made solely via automated decision-making technologies.

#### INTERNATIONAL TRANSFER OF PERSONAL DATA

As described above in this Notice, due to our global nature, it may be necessary for Signify to transfer your data internationally to Signify Affiliates (including, but not limited to Signify Netherlands B.V. in the Netherlands, and other Signify Affiliates) and trusted third parties located outside of China (e.g. Workday ([www.workday.com](http://www.workday.com)), Microsoft Office ([www.office.com](http://www.office.com)), SAP ([www.sap.com](http://www.sap.com))). When you provide Personal Data to us as part of the recruitment process, we infer your consent to transfer such Personal Data outside of China for the purposes mentioned in this Privacy Notice. The purpose, scope, method, as well as the data recipient of the transfer of your data, may vary depending on which product or service you use and/or how you interact with us. You can always contact us via the contact details in the section “What are your Privacy Rights?” described above to get more details about how we transfer your Personal Data internationally.

For transfers of Personal Data outside China, Signify will, (i) provide you with the necessary information about the cross-border transfer and obtain your separate consent, where necessary, (ii) adopt necessary measures to ensure that the overseas recipients can provide the same level of protection as required under the PIPL including entering into standard contractual clauses with the overseas recipient specifying the rights and obligations of the respective parties, applying for certification with qualified institutions, or where applicable, fulfil the security assessment process of the competent authorities.

If you wish to exercise your rights in relation to your Personal Data with us or have any questions in relation to this Privacy Disclosure, please contact us via the contact details in the section “What are your Privacy Rights?” described above.

#### WHEN WILL THERE BE UPDATES TO THIS PRIVACY NOTICE?

This Notice might change from to time.



The most current version of this Notice will govern our use of your Personal Data and can be found on the website of the [Signify Privacy Center](#), see “Legal information” section. If we make any significant changes to our privacy notice, we will take additional steps to inform you of these.

We will keep prior versions of this privacy notice in an archive for your review.

- Signify -