Privacy Policy

Document Control Information			
Version	6.0	Author	GDPRLocal
Reviewer	Signify Technology Group Ltd.	Review Date	07/10/2025
Review Frequency	12 months	Next Review Date	10/2026

Introduction

This website https://www.signifytechnology.com/ is owned and operated by Signify Technology Group Ltd. Signify Technology Group Ltd. is located at First Floor, 3 Moorgate Place, London, EC2R 6EA.

This Privacy Policy not only clarifies how we use the information when you visit our website, but also details how we collect, process, and share your personal information. This applies not just to us as Signify Technology Group Ltd. but also to our comprehensive approach in providing services and managing personal data for our clients.

This Privacy Policy not only applies to individual users but also extends to companies that use our services. We are fully committed to ensuring GDPR compliance as we deliver our services to client companies. As the data controller, we prioritise the protection of our clients' personal data, adhering to GDPR principles and legal requirements while maintaining complete transparency.

Safeguarding your privacy is our top priority, and Signify Technology Group Ltd. is dedicated to following current laws and best practices. This includes compliance with applicable data protection and privacy laws, including the General Data Protection Regulation (GDPR) and relevant United States privacy laws such as the California Consumer Privacy Act (CCPA), other state privacy regulations, and applicable federal U.S. privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA), where relevant.

Signify Technology Group Ltd. acts both as a Data controller and Data processor and is deeply committed to upholding individuals' rights in accordance with GDPR. If you have any questions or concerns regarding your privacy or data protection, please don't hesitate to reach out to our Data Protection Lead, Lauren Palmer, at:

Name: Lauren Palmer
Company name: Signify Technology Group Ltd.
Email: gdpr@signify-tech.com

How This Policy Works

This document is organised into several sections. All sections outline our overall approach to data collection, storage, and processing. Subsequent sections detail specific regulations that apply depending on your location or the use of our services. (General PP and what it includes)

To gain a comprehensive understanding of how we handle your data and ensure that we uphold your rights under relevant data protection regulations, we recommend reading the first section and any sections applicable to your situation.

In cases where our general guidelines may differ somewhat from territorial regulations, the specific territorial clauses take precedence. Nevertheless, rest assured that we prioritise your privacy and are committed to respecting your rights as dictated by applicable regulations. We are dedicated to addressing any inquiries, complaints, or concerns in a professional and timely manner.

Common Clauses and Definitions

GDPR - Whenever the terms 'The General Data Protection Regulation' or 'GDPR' are referred to in this document, it pertains to both The Regulation (EU) 2016/679 (EU GDPR) and The Data Protection Act 2018 (UK GDPR). Should there be a need to invoke other regulations, they will be appropriately and distinctly named.

The Regulation (EU) 2016/679 (EU GDPR) Territorial scope - The territorial scope of the GDPR encompasses the processing of personal data by entities established within the European Union/UK, regardless of where the processing occurs, as well as entities outside the EU/UK that either offer goods or services to individuals within the EU or monitor their behavior within the Union. It also applies in situations governed by a Member State's public international law. This means the GDPR's reach extends beyond the EU's borders, affecting organisations globally that interact with EU residents.

The Data Protection Act 2018 (UK GDPR) Territorial Scope - The UK GDPR, which came into effect post-Brexit, maintains similar territorial principles. It applies to the processing of personal data by entities established within the United Kingdom. For entities outside the UK, the UK GDPR applies if they offer goods or services to, or monitor the behaviour of, individuals within the UK. It also captures situations dictated by UK international law.

Personal data - As defined by the GDPR and other data protection legislation, personal data refers to any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. This broad definition encompasses a wide range of information, including but not limited to, names, addresses, email addresses, identification numbers, IP addresses, and cookie identifiers.

Sensitive Type of Data - Under the General Data Protection Regulation (GDPR), 'sensitive data' is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

US Privacy Laws – Whenever the term 'US Privacy Laws' is referred to in this document, it pertains collectively to the primary federal and state-level privacy and data protection frameworks applicable within the United States. These include, but are not limited to, the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act (VCDPA), the Colorado Privacy Act (CPA), the Connecticut Data Privacy Act (CTDPA), and the Utah Consumer Privacy Act (UCPA), as well as applicable federal privacy laws such as HIPAA, COPPA, and GLBA. Should there be a need to invoke other federal or state-specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), or the Gramm-Leach-Bliley Act (GLBA), they will be appropriately and distinctly named.

Territorial Scope – The territorial scope of US Privacy Laws generally encompasses entities that collect, process, or sell the personal information of residents within a given state, regardless of whether the entity itself is physically established within that state. For example, the CCPA/CPRA applies to businesses operating in or targeting California residents, provided they meet specific thresholds relating to annual gross revenue, volume of personal information processed, or percentage of revenue derived from the sale of personal information. Similarly, other state privacy laws extend their reach to organizations outside their borders if they offer goods or services to, or monitor the behavior of, residents within the respective state. Federal laws such as HIPAA, COPPA, and GLBA apply across the U.S. where relevant, independent of state residency.

Personal Information – As defined by the various US Privacy Laws, personal information refers to any information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, to a particular consumer or household. This broad definition encompasses, but is not limited to, names, postal addresses, email addresses, account identifiers, IP addresses, browsing history, and transaction data. Certain categories of information, such as publicly available or de-identified data, are expressly excluded from this definition. Federal laws may define certain categories differently, e.g., HIPAA defines health information specifically, and GLBA defines financial information.

Privacy Statement

This Privacy Policy ("Policy") explains how your information is collected, used and disclosed by Signify Technology Group Ltd. ("We" or "Us" or "our"). This policy applies where we are acting as a Data Controller, where we determine the purposes and means of the processing of that personal data, for example with respect to the personal data of our website visitors, service users, clients, partners etc.

Privacy Statement Summary:

Who will use my data?	Signify Technology Group Ltd.
Who are we?	Signify Tech is a recruitment company that provides its services to world-leading brands for everything Functional Programming related. We partner with some of the world's most exciting brands, having

	cultivated long-standing relationships that support their growth strategies by attracting, engaging, and retaining the best tech talent within Scala, Rust, Go and beyond. At Signify, we're more than recruiters; we help companies elevate their projects, enhance their teams, and exceed their goals with Signify by their side. As such, we process data in order to provide our services as a recruitment agency and meet our contractual obligations to both prospective employers and candidates for any roles. We will store and process your data in order to allow us to provide our services to you. We will also send any relevant details to authorities such as HMRC, Inland Revenue and any other organisation that requires them by law.
What for?	As a recruitment company, we collect and process data in order to provide comprehensive and effective talent solutions to our clients. At Signify Technology Group Ltd., we collect and process the data for the following purposes ● Processing for job applications in partnership with our clients, on whose behalf we are instructed to advertise job vacancies – this means that if a data subject applies for a specific job, we may pass their details on to the relevant client to proceed with the application. ● Providing our services to the clients - in order to provide our services as a recruitment company and provide them with information about potential candidates. ● Providing our services to the candidates - to match the candidates with appropriate job openings and potential employers. ● Customer and product support - providing our users with customer and product support, and monitoring the quality and types of support we provide to our users. Additionally, we may process data for administrative and operational purposes, such as managing our website, communicating with individuals who have contacted us, and complying with legal or regulatory requirements. We take data privacy and security seriously and ensure that all data we process is done so in accordance with applicable laws and regulations. We always strive to be transparent about our data processing practices and to provide individuals with clear information about their rights in relation to their personal data.

What will happen if I contact you?	If you contact us, you will be connected with our team of experienced professionals who will assist you with your talent advisory and recruitment needs. We will engage in a conversation to understand your specific requirements, whether you are a potential client seeking talent solutions for your organisation or a candidate looking for new career opportunities. Based on your needs, we will provide information about our services, including executive search, interim solutions, and consulting, and how we can tailor these services to meet your objectives. Our team will guide you through our process, answer any questions you may have, and discuss the next steps. Our goal is to ensure that your experience with us is informative, professional, and aligned with your specific talent strategy or career aspirations. If you are a candidate looking for a job, we will assess your profile and match you with suitable job opportunities based on your experience, skills and interests. We will also provide you with support and guidance throughout the recruitment process, from preparing your CV and interview coaching to negotiating job offers. If you are a client looking for top talent in the industry, we will work with you to understand your business needs and provide you with a bespoke recruitment solution to meet your specific requirements. We will also help you to identify and attract top talent from the industry and manage the recruitment process from start to finish.
What data will be stored?	At Signify Technology Group Ltd., the data we store typically includes personal and professional information that is relevant to our recruitment services. This includes details such as your name, contact information, professional qualifications, work history, and other data necessary for us to offer our services. We focus on storing data that is necessary for understanding your professional profile or organisational needs, which enables us to provide tailored talent solutions. We are committed to storing this data securely and in compliance with data protection laws, ensuring that your personal information is handled with the utmost care and respect for your privacy. The specific data we store may vary depending on the nature of our engagement with you, but typically includes the following: - Candidate data: If you are a candidate, we will store information about your skills, experience, education, employment history, and other relevant details that are necessary to match you with suitable job opportunities. - Client data: If you are a client, we will store information about your business needs and requirements, as well as information about the job opportunities you are looking to fill.

	- Contact information: We will store your name, email address, telephone number, and other contact details that you provide to us when you contact us. - Website usage data: If you visit our website, we may store information about your IP address, browser type, and the pages you visit. We may also use cookies to store additional information, such as your preferences and interests. - Other data: We may also store other data that is relevant to our engagement with you, such as records of our communications, CVs, resumes, and other documents that you provide to us. We take data privacy and security seriously and ensure that all data we store is done so in accordance with applicable laws and regulations. This includes compliance with the GDPR and applicable United States privacy laws.. We also provide individuals with clear information about our data storage practices and their rights in relation to their personal data.
What data will be shared?	The data that we share is primarily the professional information of candidates with our clients, and vice versa, as part of our recruitment services. This includes sharing candidates' professional qualifications, work experience, skills, and other relevant information that is necessary for assessing their suitability for specific roles or opportunities. We may share data in a number of circumstances in order to provide our recruitment services to clients and candidates. The specific data we share may vary depending on the nature of our engagement with you, but typically includes the following: - Candidate data: If you are a candidate, we may share information about your skills, experience, education, employment history, and other relevant details with our clients in order to match you with suitable job opportunities. - Client data: If you are a client, we may share information about your business needs and requirements with potential candidates in order to attract top talent from the industry. We take data privacy and security seriously and ensure that all data we share is done so in accordance with applicable laws and regulations. We also provide individuals with clear information about our data-sharing practices and their rights in relation to their personal data.
Who do we share data with?	The data we collect is primarily shared within the specific context of our recruitment services. We share candidate data with our clients who are looking to fill specific roles within their organisations. This

	data sharing is essential for matching the right talent with the right opportunities. Additionally, we may share data with third-party service providers who assist us in our operations, such as data analysis and processing tools. In such cases, these third parties are carefully selected and bound by confidentiality agreements and compliance with data protection laws. We are committed to ensuring that any data sharing is conducted with the utmost respect for privacy, confidentiality, and in accordance with relevant data protection regulations. Our goal is to share data only to the extent necessary for providing high-quality, tailored talent solutions. We may share your data with third-party vendors, consultants, and other service providers in order to perform tasks on our behalf. These third parties are website analytics companies, payment processing providers, CRM services providers, and email service providers. In addition, we might share your information with legal and regulatory authorities if required by law or if necessary to protect our legal rights or the rights of others.
How long?	Your data will be retained depending on the purpose for which it was collected and our legal and regulatory obligations. We keep personal data for as long as necessary to fulfil the purposes for which it was collected, including for the provision of our recruitment services, and as required to comply with our legal obligations, resolve disputes, and enforce our agreements. Once the data is no longer needed for these purposes, we take steps to securely delete or anonymise it. We regularly review our data retention policies to ensure they comply with applicable laws and align with best practices, ensuring that personal data is not kept longer than necessary. For more information, please contact us about our Data Retention Policy.
Who can access my data?	Access to your data is strictly controlled and limited to those who require it for the purpose of providing our recruitment services. This includes our team of professionals involved in executive search, talent management, and consulting services. They access your data to perform their job functions, such as matching candidates with suitable opportunities or assisting clients with their talent needs. Additionally, your data may be accessed by our clients when we share your professional information with them for potential employment opportunities. We also ensure that any third-party service providers

	who assist us in processing data are bound by confidentiality agreements and comply with our data protection standards. We maintain robust security measures and protocols to ensure that your data is protected from unauthorised access or disclosure. Our commitment is to ensure that your data is accessed only by authorised personnel and used solely for the intended professional purposes. We will never sell, share or otherwise distribute your data to any other third party other than as described here. We will share your information with any regulator or legal body that requests it, as well as any parties relevant to the process described above.
How is my data kept secure?	Keeping your data secure is a top priority for us. We employ a range of security measures to protect your data from unauthorised access, disclosure, alteration, or destruction. These measures include advanced technological solutions such as encryption, secure servers, and firewalls to safeguard the digital integrity of your data. In addition to technological measures, we have strict organisational procedures in place. Our employees are trained in data protection and confidentiality, and access to personal data is limited to those who need it to perform their job functions. We also regularly review and update our security practices to address new and emerging threats. Furthermore, we ensure compliance with relevant data protection laws and regulations, including the GDPR, and applicable United States privacy laws, where relevant to our processing activities.We are committed to continuously improving our data security measures to provide the highest level of protection for your personal information.

About This Privacy Policy

This policy sets out how we will collect, store and process the information that you provide to us, information we collect as a result of our interaction, the information we collect about you from other sources, or information we service about you by using the information we hold.

This policy helps to protect us from data security risks, including breaches of confidentiality, failing to offer choice, reputational damage, and any other risks inherent in the collection, storage, or processing of your data.

With this policy, we will work towards meeting the following goals:

- Ensuring the protection of the individual's privacy rights and personal information
- Promoting transparency and accountability in the processing of personal information
- Minimising the risk of data breaches and unauthorised access to personal information
- Compliance with applicable laws, regulations, and guidelines — including the GDPR and applicable United States privacy laws and state privacy regulations, where relevant

- Establishing a framework for effective management of personal information

Principles of Processing Personal Information

The General Data Protection Regulation (GDPR) describes how organisations must collect, handle, process, and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. GDPR is underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than is necessary
- Processed in accordance with the rights of the data subjects
- Be protected in appropriate ways
- Not be transferred outside the UK, unless that country or territory also ensures an adequate level of protection

We take these responsibilities seriously, this document describes our approach to data protection.

This policy helps to protect us from data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.
- Any other risks inherent in the collection, storage, or processing of your data

Who We Are And How To Contact Us

Signify Tech is registered in the United Kingdom and is registered with the Information Commissioner's Office. The data protection lead is Lauren Palmer. You can contact us in any of the following ways:

Name: Lauren Palmer
Company name: Signify Tech LTD
Email: gdpr@signify-tech.com

Address: First Floor, 3 Moorgate Place, London, EC2R 6EA
Number: +44 (0)203 865 0621

Our EU Representative

Under Article 27 of the GDPR, we have appointed an EU Representative to act as our data protection agent. Our nominated EU Representative is: Instant EU GDPR Representative Ltd

Adam Brogden
contact@gdprlocal.com
Tel + 353 15 549 700
INSTANT EU GDPR REPRESENTATIVE LTD
Office 2, 12A Lower Main Street, Lucan Co., Dublin K78 X5P8, Ireland

Our Data Protection Officer
Due to the nature of our business and our processing activities, we are qualified to appoint a Data Protection Officer, as stipulated in Article 37 of the GDPR.

Our DPO is:

GDPR Local Ltd
Adam Brogden
dpo.support@gdprlocal.com
Tel + 441 772 217 800
GDPR Local Ltd
1st Floor Front Suite 27-29 North Street, Brighton, England BN1 1EB

Who This Policy Applies To

This policy relates to data subjects of Signify Tech, including clients (potential employers), candidates, workers and employees, and all other individuals. Processing of your data is required in order to offer you our recruitment and selection services. This policy applies to individuals who have shared their data with Signify Tech, either as a customer, candidate, employee, supplier or in any other capacity.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This policy also applies where U.S. privacy laws are relevant and applicable state privacy regulations, to ensure that individuals' rights and protections are respected in accordance with those laws.

This can include:

- Names of Individuals
- Contact details
- Postal addresses

- Email Addresses
- Telephone numbers
- Racial, Gender Identity, Sexual Orientation or Ethnic Origin, especially in the context of our diversity, equity and inclusion initiatives. (Voluntarily provided from your end);
- Biometric data might be collected via voice recognition data, during interviews with our candidates;
- Health Data, potentially relevant in leadership coaching or executive health and well-being programs. This could include data related to mental health, stress levels, or other health-related metrics;
- Data related to disabilities or accommodations;
- Billing and payment information;
- Attendance records for events or webinars hosted by Signify Technology Group Ltd.
- Photographs or video footage from events or company premises;
- Professional qualifications and educational background;
- Employment history and work experience;
- Skills, competencies, and areas of expertise;
- Information obtained through background checks, where applicable and in compliance with legal requirements;
- And other information as required.

What this policy applies to

This section describes the lawful basis for processing your data and applies to the information about yourself that you choose to provide us with or that you allow us to collect. This includes:

- The Information you provide when you contact us
- Data you provide when you participate in our surveys or feedback forms;
- Details you share during events, webinars, or workshops that we organise or participate in;
- Information collected through our customer support channels when you seek assistance;
- Information regarding your preferences, including the settings you choose within our platforms or applications;
- Your communications and interactions with us on social media platforms;

- Information we collect about how you use the website
- Information relating to products and services we offer to you and other transactions including financial and other personal information required to complete these transactions
- Information that is given and stored as part of our ongoing relationship
- Information we collect from other sources such as the internet, social media, commercial databases, other companies, and other third parties
- Information we collect from our conferences
- Data we acquire from partners or third parties who have your consent to share it with us

We do not routinely collect or process sensitive data about you; however, where this is the case, we will ensure we take appropriate precautions to protect your data.

How your information will be used - Our Lawful Basis

We will only use your personal data for the purposes for which we collected it and as you would reasonably expect your data to be processed and only where there is a lawful basis for such processing, for example:

Purpose/Activity	Type of data	Lawful basis for processing
To register you as a new client	(a) Identity (b) Contact	a. Performance of a contract with you. b. Consent
To register you as a new candidate	a. Identity b. Contact c. Professional qualifications and educational background d. Employment history and work experience e. Skills, competencies, and areas of expertise	a. Consent b. Legitimate Interest
To process and deliver our services, you request, including recruitment and employment services, managing payments, fees and charges	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you. (b) Necessary for our legitimate interests to recover debts owed to us (c) Consent
To manage our ongoing	(a) Identity	(a) Performance of a contract

relationship with you which will include notifying you about changes to our terms, recruitment services, or privacy policy, to maintain our records	(b) Contact (c) Profile (d) Marketing and Communications	with you, (b) Necessary to comply with a legal obligation, (c) Necessary for our legitimate interests to keep our records updated and to study how customers use our products/services (d) Consent
To administer and protect our business and our site (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise (b) Necessary to comply with a legal obligation (c) Consent
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	(a) Technical (b) Usage	(a) Necessary for our legitimate interests to define types of customers for our products and services, to keep our site updated and relevant, to develop our business and to inform our marketing strategy (b) Consent
To make suggestions and recommendations to you about goods or services that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile	(a) Necessary for our legitimate interests to develop our products/services and grow our business (b) Consent
To conduct background checks for candidates	a. Identity b. Employment history c. Reference	a. Consent b. Necessary for our legitimate interests to ensure the reliability of candidates
To provide personalised career guidance and	a. Identity b. Contact	a. Consent b. Legitimate Interest

support	c. Professional qualifications and educational background d. Employment history and work experience e. Preferences and Interests	
To facilitate networking opportunities and professional connections	a. Identity b. Contact c. Professional qualifications and educational background d. Employment history and work experience	a. Consent b. Necessary for our legitimate interests to provide value-added services
To conduct surveys and collect feedback for service improvement	a. Identity b. Contact c. Opinions and feedback	a. Consent b. Necessary for our legitimate interests to improve services and customer satisfaction
To comply with legal and regulatory requirements	a. Identity b. Contact c. Financial d. Transaction e. Legal documents	a. Necessary to comply with a legal obligation
To provide updates and newsletters about industry trends and company news	a. Identity b. Contact c. Marketing and Communications preferences	a. Consent b. Necessary for our legitimate interests to engage with our audience and inform them about our sector
To facilitate participation in webinars, workshops, and events	a. Identity b. Contact c. Preferences and interests	a. Performance of a contract with you b. Consent c. Legitimate Interest

For U.S. residents: Please see appendix 1: U.S. Privacy notice and categories of Personal Information.

We will use your data for the purpose it was collected and where we have your consent or an appropriate lawful basis we may use your personal information to provide you with marketing information about services, promotions and offers that may be of interest to you. This document explains how you can change whether to receive this information. Please note that, even if you choose not to receive this information, we may still use your personal information to provide you with important services communications, including communications in relation to any services we provide to you.

You will only receive marketing communications from us if you have:

- Requested information from us;
- If you provided us with your details and ticked the box at the point of entry of your details for us to send you marketing communications;
- You have not opted out of receiving marketing;
- Where we have an appropriate lawful basis.

We will get your express opt-in consent before we use or share your personal data with any third party for marketing purposes.

How to change your preferences

We operate in line with GDPR data protection guidelines. We respect your rights and will respond to any request for access to personal information and requests to delete, rectify, transfer, data and to stop processing. We will also advise you on how to complain to the relevant authorities, namely the Information Commissioner's Office.

Any requests or objections should be made in writing to the Data Controller or you can visit our website, call, or email us to contact us to change your preferences at any time.

Opting out at a later date

Where you give your consent for us to process your data, for example when you agree to us sending you marketing information or where you agree to us processing financial data, you can contact us to amend or withdraw your consent at any time. You can also choose to object to processing and request deletion of your data. We respect all user rights as defined in GDPR.

If you have any comments or wish to complain, please contact us.

How we store and process your data

Your data will be collected, stored and processed primarily in the UK, where we transfer your data outside the UK, we ensure that appropriate technical and organisational safeguards are in place to protect your data. Your data will normally be stored for as long as necessary in order to meet our legal obligations and protect our interests. For more information, please contact us about our Data Retention Policy.

In order to provide our services we may use carefully selected third parties. These third parties may operate outside the UK, if this is the case we will ensure we have in place appropriate safeguards to protect your data.

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to find out more about how the processing for the new purpose is compatible with the original purpose, please email us. If we need to use your personal data for a purpose unrelated to the purpose for which we collected the data, we will notify you and we will explain the legal ground of processing.

We may also use recognised third parties to take payment, conduct credit reports and other checks, manage our company accounts and provide banking services. We will store transactions, payment and order data for up to 7 years or for as long as required by UK financial and company regulations. These third parties may operate outside the UK, if this is the case we will ensure we have in place appropriate safeguards to protect your data.

We may be legally obliged to disclose your personal information without your knowledge to the extent that we are required to do so by law; in connection with any ongoing or prospective legal proceedings; in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk); to any person who we reasonably believe may apply to a court or other competent authority for disclosure of that personal information where, in our reasonable opinion, such court or authority would be reasonably likely to order disclosure of that personal information.

Your rights under GDPR

Under the GDPR, or the Data Protection Act 2018 in the UK, you have:

- The right of access to the data - You have the right to obtain confirmation as to whether personal data concerning you is being processed, and, where that is the case, access to that personal data. Reasonable access to your personal data will be provided at no cost. If access cannot be provided within a reasonable time frame, We will provide you with a date when the information will be provided. If, for some reason, access is denied, we will provide an explanation as to why access has been denied.
- The right of rectification - You have the right to request the rectification of any inaccurate or incomplete personal data concerning yourself.
- The right to "be forgotten"/ Right of erasure - This refers to your right to have your personal data deleted from our database, including from any third parties who may have access to that data. However, where there are legal requirements for us to store the data for a certain period of time, related to our business, which includes elements of your personal data, we will not be able to delete that data until after the statutory retention period.
- The right to restrict the processing of your data - You have the right to ask us to restrict the processing of your personal data where you challenge the accuracy of the personal data we are storing; We no longer need your personal data for the purposes of the processing, or you have objected to processing.
- The right to object to processing – You have the right to object to the processing of your personal data.
- The right to Data portability - You have the right to receive the personal data concerning you, which you provided to us, in a structured, commonly used and machine-readable format.
- Rights related to automated decision-making, including profiling.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

For questions or complaints concerning the processing of your personal data, you can email us at gdpr@signify-tech.com or dpo.support@gdprlocal.com

If you are a resident of a U.S. state with privacy legislation, please see Appendix 1 for details of your rights under U.S. privacy laws.

Our obligations

We take responsibility for the management and security of your personal data extremely seriously. In accordance with the General Data Protection Regulation, acting as a data controller and data processor, we follow the key principles of data protection. These require that personal data be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and kept up to date. Every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
- Kept for no longer than is necessary for the purposes for which the personal data is processed;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Third Parties

We may have to share your personal data with selected third parties in order to meet our obligations to you and for the purposes described in this document:

- For candidates/workers - Prospective employers and companies that may offer you work, and other relevant third parties
- For clients – Candidates / employees / workers that may be interested in any vacancies and other relevant third parties

For all users of our site:

- Service providers who provide IT and system administration services.
- Third parties including data processors, suppliers, service providers, equipment

providers, and other third parties as required to run and grow our business;

- Professional advisers including lawyers, bankers, auditors and insurers who provide consultancy, credit scoring, banking, legal, fraud protection, insurance and accounting services etc.
- Other technology companies providing tracking, analytics, and advertising companies;
- HM Revenue & Customs, regulators and other authorities based in the United Kingdom and other relevant jurisdictions who require reporting of processing activities in certain circumstances.
- Government organisation, regulators, other legal authorities and other relevant jurisdictions who require reporting of processing activities in certain circumstances;
- Third parties to whom we sell, transfer, or merge parts of our business or our assets;
- Recruitment partners and job boards to broaden the scope of our executive search and talent acquisition services;
- Other companies as required to meet our obligations to you and run our business

We require all third parties to whom we transfer your data to respect the security of your personal data and to treat it in accordance with the law. We only allow such third parties to process your personal data for specified purposes and in accordance with our instructions.

Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know such data. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

Where required under GDPR, we will report any breaches or potential breaches to the appropriate authorities within 24 hours and to anyone affected by a breach within 72 hours. If you have any queries or concerns about your data usage, please contact us.

Our website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

Processing of children's information

We do not knowingly collect or maintain personal data from anyone under the age of 13, unless or except as permitted by law. Any person who provides personal data through the Website represents to us that he or she is 13 years of age or older. If we learn that personal data has been collected from a user under 13 years of age on or through the Website, then we will take the appropriate steps to cause this information to be deleted.

If you are the parent or legal guardian of a child under 13 who has become a member of the Website or has otherwise transferred personal data to the Website, please contact the Company using our contact information below to have that child's account terminated and information deleted.

Cookies

A cookie is a small file that asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences. We use traffic log cookies to identify which pages are being used. This helps us analyse data about webpage traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes, and then the data is removed from the system.

Overall, cookies help us provide you with a better website by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser settings to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

As well as your ability to accept or reject cookies, we also require your permission to store cookies on your machine, which is why when you visit our site, you are presented with the ability to accept our terms of use, including the storage of cookies on your machine.

Contacting us, exercising your information rights and Complaints

If you have any questions or comments about this Privacy Policy, wish to exercise your information rights in connection with the personal data you have shared with us or wish to complain, please contact Operations at Signify Technology.

We aim to process data protection requests within 30 days, SAR responses are usually free, but we reserve the right to charge for excessive or unfounded requests. We fully comply with Data Protection legislation and will assist in any investigation or request made by the appropriate authorities.

If you remain dissatisfied, then you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at:

Information Commissioner's Office
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF,
www.ico.org.uk

Appendix 1: U.S. Privacy notice and categories of Personal Information

Effective date: [10/07/2025]

Last updated: [10/2026]

Notice at Collection for U.S. Residents

This section applies to individuals residing in the United States and is provided in accordance with applicable U.S. state privacy laws, including the California Consumer Privacy Act (CCPA/CPRA) and similar privacy regulations in states such as Virginia Consumer Data Protection Act (VCDPA), Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CTDPA), Utah Consumer Privacy Act (UCPA), and Texas Data Privacy and Security Act (TDPSA). Unless otherwise defined here, all terms used in this Appendix have the meanings given in the respective laws.

It explains the categories of personal information we collect, the purposes for which we use it, and your privacy rights.

We collect and use the categories of personal information listed in the table below for the business purposes described in this Privacy Policy, such as providing recruitment and talent advisory services, maintaining client and candidate relationships, managing our website, and complying with legal obligations.

We do not sell or share personal information for monetary value or for targeted advertising purposes. You have the right to request access to, correction of, or deletion of your personal information, as well as to opt out of any data sharing, limit the use of sensitive personal information, or appeal a decision regarding a privacy request. You may exercise these rights by contacting us at privacy@signify-tech.com.

Categories of Personal Information We Collect

Category of Personal Information	Types of data	Sources	Purpose of processing	Categories of recipients	Retention period / criteria

Identifiers	Name, email address, telephone number, mailing address, online identifiers (e.g., IP address)	Directly from you; automatically via our website	To communicate with you, provide recruitment services, maintain our business relationship	Internal staff, clients (for recruitment), IT and CRM service providers	Typically retained for up to 7 years after last interaction, or as required by law
Professional or Employment-Related Information	Job title, CV/resume, work history, qualifications, references	Directly from you; from third-party job platforms or referrals	To assess candidate suitability, match candidates with opportunities, and support clients' hiring needs	Internal recruitment consultants, client companies	Up to 7 years following the end of the recruitment process or placement
Education Information	Degrees, certifications, training records	Directly from you; from your CV/resume	To evaluate candidate qualifications and present profiles to clients	Clients (employers)	Up to 7 years following collection
Internet or Other Electronic Network Activity Information	IP address, browser type, device information, website activity, cookie preferences	Automatically collected through our website	To operate, secure, and improve our website; analytics and site functionality	IT service providers, analytics providers	Typically 2 years or until cookies are deleted/opted out

Commercial Information	Records of services requested, purchased, or considered	Directly from clients and candidates	To manage business relationships and provide recruitment services	Internal staff, CRM providers	Up to 7 years for accounting and compliance purposes
Sensitive Personal Information (if provided voluntarily)	Diversity data (e.g., race/ethnicity), health/disability information for accessibility, background checks	Directly from you (voluntary disclosure)	To comply with equal opportunity and accessibility obligations	Clients (employers) only where required or permitted by law	Retained only as necessary for recruitment or compliance purposes, then deleted or anonymized
Inferences Drawn from Personal Information	Professional suitability profiles, preferences, skill assessments	Derived internally based on your interactions and information provided	To match candidates to roles and improve recruitment services	Internal staff, client companies	Retained in line with candidate data (up to 7 years)

Use of Personal Information

We use personal information for the same purposes described in our main Privacy Policy and for the operation of our recruitment and talent-matching services. Specifically, we may use your personal information for the following purposes:

- **Recruitment and placement services:**
  To process job applications and match candidates with suitable roles, including sharing candidate details with clients for positions they have applied for or that may be relevant to their experience and interests.

- **Client services:**
  To provide recruitment and talent-sourcing services to our clients, including communicating about potential candidates and maintaining ongoing business

relationships.

- **Candidate services:**
  To support and guide candidates through the recruitment process, communicate about opportunities, and provide updates regarding applications or future roles.

- **Customer and product support:**
  To provide customer support to users of our website and services, monitor and improve the quality of support, and resolve technical or service-related issues.

- **Service improvement and analytics:**
  To analyze service usage, improve our recruitment processes, website, and communication tools, and develop new features to enhance user experience.

- **Administrative and operational purposes:**
  To manage our business operations, maintain accurate records, and ensure the proper functioning and security of our website and systems.

- **Legal and regulatory compliance:**
  To comply with applicable legal, regulatory, or contractual obligations, including record-keeping and responding to lawful requests.

We take data privacy and security seriously and ensure that all processing of personal information is conducted in accordance with applicable data protection laws and with appropriate safeguards in place.

Your Rights Under U.S. Privacy Laws

Under applicable U.S. privacy laws, including the California Consumer Privacy Act (CCPA, as amended by the California Privacy Rights Act - CPRA) and other state privacy regulations, you have the following rights:

- Right to Know / Access – You have the right to request that we disclose the categories and specific pieces of personal information we have collected about you, the sources from which it was collected, the purposes for which it is used, and the categories of third parties with whom it is shared.

- Right to Delete – You have the right to request the deletion of personal information that we have collected about you, subject to certain exceptions under law (e.g., legal

obligations, fraud prevention, or completing a transaction).

- Right to Correct / Rectification – You have the right to request that we correct any inaccurate personal information we hold about you.

- Right to Opt-Out of Sale or Sharing – While we do not sell or share personal information for monetary value or for targeted advertising purposes, if you reside in California or other U.S. states with similar laws, you have the right to direct us to opt out of any sale or sharing of your personal information where applicable.

- Right to Limit Use of Sensitive Personal Information – If applicable under CPRA, you may limit the use of your sensitive personal information for purposes beyond providing our services. We do not use or disclose sensitive personal information for purposes unrelated to service provision without your consent.

- Right to Non-Discrimination – We will not discriminate against you for exercising your privacy rights. This means we will not deny you services, charge you a different price, or provide a lesser quality of service because you have exercised your rights. Certain impacts may occur if data is deleted, but these are related to service functionality, not punitive action.

- Other U.S. State Privacy Rights – If you reside in a state with its own privacy law (such as Virginia, Colorado, Connecticut, Utah, and others), you generally have similar rights to access, correct, delete, obtain portability, and opt out of certain processing. If a request is denied under any state law, we will inform you how to appeal our decision.

We may need to request specific information from you to help us confirm your identity and ensure your right to exercise these rights. This is a security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Authorized agents may submit requests on your behalf if they provide proof of authorization.

We aim to respond within 45 days, extendable by an additional 45 days if reasonably necessary.

For questions, requests, or complaints concerning the processing of your personal information under U.S. privacy laws, you can contact us at: privacy@signify-tech.com or our Data Protection Lead at dpo.support@gdprlocal.com**.**

Security

We have implemented appropriate technical and organizational security measures to protect your personal information from unauthorized access, disclosure, alteration, or destruction.

Access to personal information is restricted to employees, agents, contractors, and other third parties who require it for legitimate business purposes, and they are bound by confidentiality obligations.

While U.S. laws generally do not prescribe a strict 72-hour notification deadline, we will notify affected individuals in a timely manner as required under applicable state law.

If you have any questions or concerns regarding the security of your information or how we handle data incidents, please contact us.

Our website may include links to third-party websites, plug-ins, and applications. Clicking on those links or enabling those connections may allow third parties to collect or share information about you. We do not control these third-party websites and are not responsible for their privacy practices. When you leave our website, we encourage you to review the privacy notice of every site you visit.

Additional Information for U.S. Residents

- We will not discriminate against you for exercising any of your privacy rights.
- We may collect limited sensitive personal information (e.g., demographic or health-related information) when voluntarily provided. We do not use or disclose such information beyond the purposes permitted under applicable U.S. privacy laws.
- Our services are not directed to children under 13. We do not knowingly collect personal information from children. If we learn that we have inadvertently collected such information, we will delete it promptly.
- Some cookies and similar technologies used on our website may qualify as “sharing” under U.S. state privacy laws. You may manage your cookie preferences through our cookie consent banner.
- You may also contact your state’s Attorney General or the Federal Trade Commission (FTC) for further information or to submit a complaint.

We may update this Appendix from time to time. The “last update” date above indicates when it was most recently revised. Material changes will be communicated via our website or direct notice where required.